9

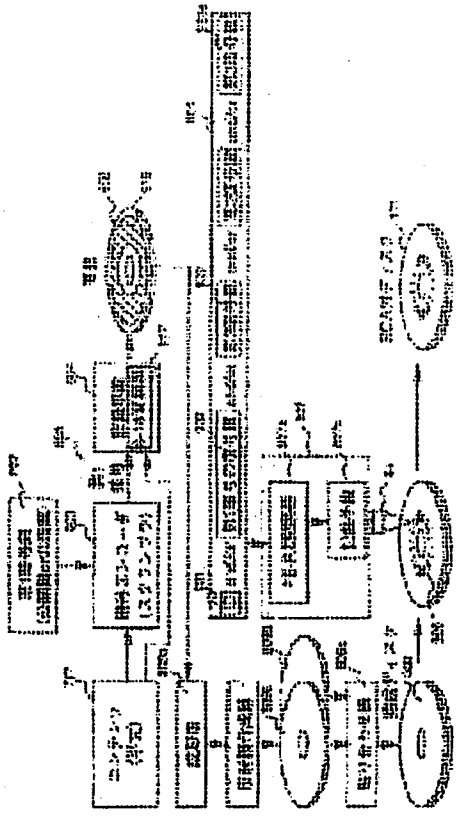
CIPHER RECORDER, CIPHER RECORDING METHOD, PROGRAM FOR MAKING COMPUTER CARRY OUT THE METHOD, AND COMPUTER READABLE RECORDING MEDIUM WITH THE PROGRAM RECORDED THEREON

Publication number: JP2002313020 (A)
Publication date: 2002-10-25
Inventor(s): OSHIMA MITSUAKI; GOTOU YOSHITOSHI; TANAKA SHINICHI; KOISHI KENJI; MORIYA MITSURO; TAKEMURA YOSHIYA +
Applicant(s): MATSUSHITA ELECTRIC IND CO LTD +
Classification:
- international: ***G06F12/14; G06F21/24; G11B20/10; G11B7/004; H04L9/32;*** **G06F12/14; G06F21/00; G11B20/10; G11B7/00; H04L9/32;** (IPC1-7): G06F12/14; G11B20/10; G11B7/004; H04L9/32
- European:
Application number: JP20020008404 20020117
Priority number(s): JP20020008404 20020117; JP19950261247 19951009; JP19960008910 19960123; JP19960211304 19960809

Also published as:
JP3786015 (B2)

Abstract of **JP 2002313020 (A)**

PROBLEM TO BE SOLVED: To simplify operation sequence or procedures for the applied system of a network using type optical disk. SOLUTION: A sub-information recording area is provided to the optical disk, and an ID or a cryptographic key or a decoding key different from a disk to a disk is recorded at a factory. Operation sequence or procedures can be obviated by a user's using the ID for deciphering software, the cryptographic key when transmitting a cipher, the decoding key when receiving a cipher, and safe distribution of information via a communication means is realized by checking the record of contents using prescribed information.



Data supplied from the ***espacenet*** database — Worldwide

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－313020
（P2002－313020A）
(43)公開日　平成14年10月25日(2002.10.25)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ１１Ｂ　20/10		Ｃ１１Ｂ　20/10	Ｈ	5Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｃ０６Ｆ　12/14	３２０Ｂ	5Ｄ０４４
			３２０Ｆ	5Ｄ０９０
Ｇ１１Ｂ　7/004		Ｃ１１Ｂ　7/004	Ｃ	5Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｂ	

審査請求　有　請求項の数10　ＯＬ　（全 30 頁）

(21)出願番号　特願2002－8404(P2002－8404)
(62)分割の表示　特願平9－511086の分割
(22)出願日　平成８年10月８日(1996.10.8)

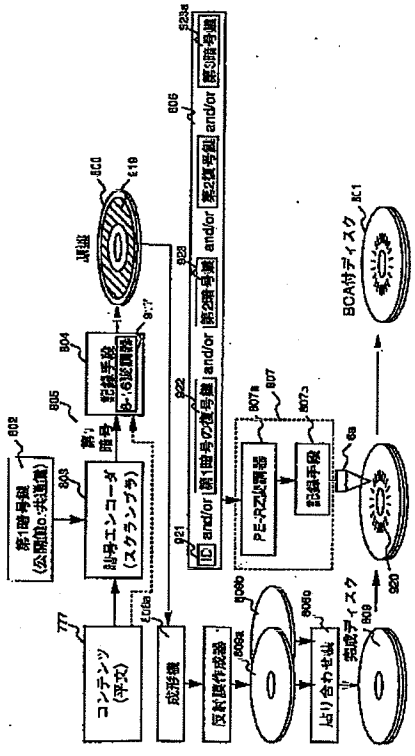
(31)優先権主張番号　特願平7－261247
(32)優先日　平成７年10月９日(1995.10.9)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平8－8910
(32)優先日　平成８年１月23日(1996.1.23)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平8－211304
(32)優先日　平成８年８月９日(1996.8.9)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　大鳴　光昭
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　後藤　芳稔
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

最終頁に続く

(54)【発明の名称】　暗号記録装置、暗号記録方法、その方法をコンピュータに実行させるプログラムおよびそのプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　ネットワーク利用型の光ディスクの応用システムの操作手順や諸手続きを簡便化する。
【解決手段】　光ディスクに副情報記録領域を設け、ディスク毎に異なるＩＤや暗号の暗号鍵や復号鍵を工場で記録しておく。使用者がソフトの暗号解除にはＩＤ、暗号送信時に暗号鍵、暗号受信時に復号鍵を用いることにより手順や手続きを省略でき、コンテンツの記録を、所定の情報を用いたチェックを行うことで通信手段を介して安全な情報配信が実現する。



【特許請求の範囲】
【請求項１】　コンテンツを入力するための入力手段と、
入力された前記コンテンツを暗号化する暗号化手段と、
暗号化された前記コンテンツを記録する記録手段と、
を備え、
前記暗号化手段と前記記録手段との間で、所定の情報を用いたチェックを行い、そのチェックが正常な場合に、前記暗号化手段で暗号化された前記コンテンツが前記記録手段に送られることを特徴とする暗号記録装置。
【請求項２】　コンテンツを受信する受信手段と、
受信された前記コンテンツを暗号化する暗号化手段と、
暗号化された前記コンテンツを記録する記録手段と、
を備え、
前記暗号化手段と前記記録手段との間で、所定の情報を用いたチェックを行い、そのチェックが正常な場合に、前記暗号化手段で暗号化された前記コンテンツが前記記録手段に送られることを特徴とする暗号記録装置。
【請求項３】　コンテンツを入力するための入力手段と、
入力された前記コンテンツを暗号化する暗号化手段と、
暗号化された前記コンテンツを記録する記録手段と、
前記暗号化手段と前記記録手段との間で、所定の情報を用いたチェックを行うチェック手段と、
を備え、
前記チェックが正常な場合に、前記暗号化手段で暗号化された前記コンテンツが前記記録手段に送られることを特徴とする暗号記録装置。
【請求項４】　コンテンツを受信する受信手段と、
受信された前記コンテンツを暗号化する暗号化手段と、
暗号化された前記コンテンツを記録する記録手段と、
前記暗号化手段と前記記録手段との間で、所定の情報を用いたチェックを行うチェック手段と、
を備え、
前記チェックが正常な場合に、前記暗号化手段で暗号化された前記コンテンツが前記記録手段に送られることを特徴とする暗号記録装置。
【請求項５】　前記所定の情報は、暗号化された前記コンテンツが記録される記録媒体に格納された情報であることを特徴とする請求項１から４の何れか１つ項に記載の暗号記録装置。
【請求項６】　前記所定の情報は、暗号化された前記コンテンツが記録される記録媒体を識別する識別情報であることを特徴とする１から４の何れか１つ項に記載の暗号記録装置。
【請求項７】　コンテンツを入力する入力工程と、
入力された前記コンテンツを暗号化する暗号化工程と、
前記暗号化を行う暗号化手段と暗号化された前記コンテンツを記録する記録手段との間で、所定の情報を用いたチェックを行うチェック工程と、
前記チェックが正常な場合に、暗号化された前記コンテンツを記録する記録工程と、
を含むことを特徴とする暗号記録方法。
【請求項８】　コンテンツを受信する受信工程と、
受信された前記コンテンツを暗号化する暗号化工程と、
前記暗号化を行う暗号化手段と暗号化された前記コンテンツを記録する記録手段との間で、所定の情報を用いたチェックを行うチェック工程と、
前記チェックが正常な場合に、暗号化された前記コンテンツを記録する記録工程と、
を含むことを特徴とする暗号記録方法。
【請求項９】　請求項７または８に記載の暗号記録方法をコンピュータに実行させるプログラム。
【請求項１０】　請求項９に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は光ディスクおよび光ディスクシステムおよび暗号通信方法に関するものである。
【０００２】
【従来の技術】近年、インターネット等のネットワークと光ＲＯＭディスクの普及に伴い、光ＲＯＭディスクを用いたネットワークソフト流通が始まりつつある。また電子商取引きの検討が進んでいる。
【０００３】従来技術として、ＣＤ－ＲＯＭをメディアとして用いたソフト電子流通システムが実用化されている。この場合パスワードを与えて、ＣＤ－ＲＯＭに予め記録され暗号化されたソフトの暗号を解くといった方法が一般的である。
【０００４】
【発明が解決しようとする課題】しかし、ＣＤ－ＲＯＭの場合、ディスク上に追記記録できないため各ディスクのＩＤは個別に設定できない。従って単純に用いれば、１つのパスワードが同一原盤から製造された全てのディスクの暗号を解除してしまう。このため、ＣＤ－ＲＯＭを用いた場合、各々のディスク個有のＩＤをパソコン側のハードディスク上に作成したり、センターで作成したＩＤを郵便によりユーザーに送るという作業が必要であった。
【０００５】従来の光ディスクや光ディスクシステムを用いた電子流通システムにおいては、光ディスクもしくはシステムにＩＤや暗号鍵を簡便に供給することが求められている。本発明はＲＯＭディスクを用いた電子流通システムにＩＤと暗号鍵の簡便な供給を実現することを目的とする。
【０００６】
【課題を解決するための手段】この課題を解決するために、光ディスクのピット部にバーコードを重ね書きした追記領域（以下ＢＣＡと略す）を設け光ディスク製造時

に、ＢＣＡ領域にディスク毎に異なるＩＤと必要に応じて通信用の暗号鍵、通信用の復号鍵暗号文の復号鍵を個別に記録しておくことにより、ディスクとユーザーに配布した時点で、ユーザーにはユーザーＩＤ番号と通信用の送信用の暗号鍵、受信用の復号鍵の３つが自動的に配布されていることになり、従来のシステムを複雑にしていたいくつかの手順が省略できる。こうして、暗号通信とコンテンツの入ったディスクの識別が同時に実現する。

【０００７】

【発明の実施の形態】実施例に基づき、本発明を説明する。なお、本文ではＢＣＡ方式を用いた追記領域をＢＣＡ領域、ＢＣＡにより記録されたデータをＢＣＡデータと呼ぶ。また第１識別情報はＩＤ、もしくはディスクＩＤとも呼ぶ。

【０００８】図１はＢＣＡ付ディスクの代表的な工程を示す。まず、公開鍵等の第１暗号鍵８０２を用いて暗号エンコーダ８０３でコンテンツ７７７が暗号化された第１暗号８０５がマスタリング装置等の８－１６変調器９１７により変調され、この変調信号がレーザーにより原盤８００の第１記録領域９１９に凹凸のピットとして記録される。この原盤８００を用いて成形機８０８ａでディスク状の透明基板９１８を成形し、反射膜作成機８０８ｂでＡ１反射膜を形成し０．６ミリ厚の片面ディスク８０９ａ、８０９ｂを作成し、貼り合わせ機８０８ｃで貼り合わせた完成ディスク８０９の第２記録領域９２０にトリミング装置８０７で、ディスクＩＤ９２１もしくは第１暗号の復号鍵９２２もしくはインターネット通信用の第２暗号鍵９２３をＰＥ変調とＲＺ変調を組み合わせたＰＥ－ＲＺ変調器８０７ａで変調し、パルスレーザー８０７ｂでＢＣＡトリミングして、ＢＣＡ付ディスク８０１を製造する。貼り合わせディスクを用いているので、中に入ったＢＣＡは改ざん出来ず、セキュリティ用途に用いることが出来る。

【０００９】説明に入る前に、ＢＣＡについて、簡単に説明する。

【００１０】図２の（１）に示すようにＢＣＡでは２層ディスク８００にパルスレーザー８０８で、アルミ反射膜８０９をトリミングし、ストライプ状の低反射部８１０をＰＥ変調信号に基づいて記録する。図２（２）に示すようにＢＣＡのストライプがディスク上に形成され、このストライプを通常の光ヘッドで再生するとＢＣＡ部は反射信号がなくなるため図２（３）に示すように変調信号が間欠的に欠落した欠落部８１０ａ，８１０ｂ，８１０ｃが発生する。変調信号は第１スライスレベル９１５でスライスされる。一方欠落部８１０ａ等は信号レベルが低いので、第２スライスレベル９１６で容易にスライスできる。図３の記録再生波形図に示す様に、形成されたバーコード９２３ａ，９２３ｂは、図３（５）に示すように通常の光ピックで第２スライスレベル９１６でレベルスライスすることにより再生可能で図３（６）に示すようにＬＰＦフィルタで波形成形されＰＥ－ＲＺ復調され、（７）に示すようにデジタル信号が出力される。図４を用いて復調動作を説明する。まず、ＢＣＡ付ディスク８０１は透明基板が２枚、記録層８０１ａが中にくるように貼り合わせてあり、記録層８０１ａが１層の場合と記録層８０１ａ，８０１ｂの２層の場合がある。２層の場合は光ヘッド６に近い第１層の記録層８０１ａのコントロールデータにＢＣＡが記録されているかどうかを示すＢＣＡフラグ９２２が記録されている。ＢＣＡは第２層８０１ｂに記録されているので、まず第１層記録層８０１ａに焦点を合わせ第２記録領域９１９の最内周にあるコントロールデータ９２４の半径位置へ光ヘッド６を移動させる。コントロールデータは主情報なのでＥＦＭ又は８－１５又は８－１６変調されている。このコントロールデータの中のＢＣＡフラグ９２２が‘１’の時のみ、１層、２層部切換部８２７で、焦点を第２記録層８０１ｂに合わせてＢＣＡを再生する。レベルスライサー５９０で図２（３）に示すような、一般的な第１スライスレベル９１５でスライスするとデジタル信号に変換される。この信号を第１復調部においてＥＦＭ９２５又は８－１５変調９２６又は８－１６変調９２の復調器で復調し、ＥＣＣデコーダ３６でエラー訂正し主情報が出力される。この主情報の中のコントロールデータを再生し、ＢＣＡフラグ９２２が１の場合のみＢＣＡを読みにいく。ＢＣＡフラグ９２２が１の時、ＣＰＵ９２３は１層、２層部切換部８２７に指示を出し、焦点調節部８２８を駆動して、第１層の記録層８０１ａから第２層の記録層８０１ｂへ焦点を切り替える。同時に第２記録領域の９２０の半径位置、すなわちＤＶＤ規格の場合はコントロールデータの内周側の２２．３ｍｍから２３．５ｍｍの間に記録されているＢＣＡを光ヘッド６を移動させ、ＢＣＡをよみとる。ＢＣＡ領域では図２（３）に示すようなエンベロープが部分的に欠落した信号が再生される。第２レベルスライサ９２９において第１スライスレベル９１５より低い光量の第２スライスレベル９１６を設定することにより、ＢＣＡの反射部欠落部は検出でき、デジタル信号が出力される。この信号を第２復調部９３０においてＰＥ－ＲＺ復調し、ＥＣＣデコーダ９３０ｄにおいてＥＣＣデコードすることにより副情報であるＢＣＡデータが出力される。このようにして、８－１６変調の第１復調器９２８で主情報をＰＥ－ＲＺ変調の第２復調部９３０で副情報つまりＢＣＡデータを復調再生する。

【００１１】図５（ａ）にフィルタ９４３通過前部の再生波形、（ｂ）に低反射部８１０のスリットの加工寸法精度を示す。スリットの巾は５～１５μｍ以下にすることは難しい。また、２３．５ｍｍより内周に記録しないと記録データを破壊してしまう。このことからＤＶＤの場合最短の記録周期＝３０μｍ、最大半径＝２３．５ｍ

mの制限からフォーマット後の最大容量は１８８ｂｙｔｅｓ以下に限定される。

【００１２】変調信号は、８－１６変調方式を用いてピットで記録されており、図５（ａ）の高周波信号部９３３のような高周波信号が得られる。一方、ＢＣＡ信号は低周波信号部９３２のような低周波信号となる。このように、主情報がＤＶＤ規格の場合、最高約４．５ＭＨｚの高周波信号９３２であり、図５（ａ）に示すように、副情報が周期８．９２μｓつまり約１００ＫＨｚの低周波信号９３３であるため、ＬＰＦ９４３を用いて副情報を周波数分離することが容易である。図４に示すようなＬＰＦ９４３を含む周波数分離手段９３４で、２つの信号を容易に分離することが出来る。この場合、ＬＰＦ９４３は簡単な構成でよいという効果がある。

【００１３】以上がＢＣＡの概略である。

【００１４】では、図６を用いて、暗号ソフト解錠システムの全体システムをパスワード発行と暗号通信と発注者の認証の動作に絞り説明する。まず、プレス工場のステップは、図１の場合とほぼ同じ手順で製造されるので、原盤８００と完成ディスク８０９の図は省略する。

【００１５】プレス工場８１１において、第１～ｎ番目のコンテンツの平文８１０は暗号エンコーダ８１２により、各々第１～ｎ番目の暗号鍵８１３でデータの暗号化又は映像信号のスクランブルがなされ、光ディスクの原盤８００に記録される。この原盤８００から、プレスされて製造されたディスク状の基板８０９に反射膜が形成された後に、２枚のディスク状の基板を貼り合わせた後、完成ディスク８０９が作られる。この完成ディスク８０９に、ディスク毎に異なるＩＤ８１５もしくは／かつ第１暗号鍵８１６（公開鍵）もしくは／かつ、第２暗号鍵８１７（公開鍵）、第２コンピュータの接続アドレス８１８がＢＣＡ領域８１４に記録されたＢＣＡ付ディスク８０１が、ユーザーに配布される。

【００１６】このディスクのコンテンツは暗号化されているので、再生するには代金等の代価を払ってパスワード発行センターつまり電子商店もしくは、モールからパスワードをもらう必要がある。この手順を述べる。

【００１７】ユーザーの第１コンピュータ９０９では配布されたＢＣＡ付ディスク８０１を再生装置８１９で再生すると、ＰＥ－ＲＺ復調部を含むＢＣＡ再生部８２０により、ＩＤ８１５、第１暗号鍵８１６、第２暗号鍵８１７、接続アドレス８１８のデータが再生される。パスワードをもらうためには、パスワード発行センター８２１のサーバーである第２コンピュータ８２１ａの接続アドレス８１８へ通信部８２２を介してインターネット等のネットワーク８２３経由で接続し第２コンピュータ８２１ａへＩＤを送信する。

【００１８】ここで、暗号通信の手順について述べる。第２コンピュータ８２１ａはユーザーの再生装置８１９からのＩＤ８１５を受信する。すると“モール”や“電子商店”とよばれるパスワード発行センター８２１の第２コンピュータすなわちサーバー８２１ａは暗号鍵データベースＤＢ８２４をもつ。このデータベースにはこのディスク個有のＩＤもしくはＩＤの第１暗号鍵８１６に対応する復号鍵である秘密鍵、つまり第１復号鍵８２５とＩＤの表が収容されている。従ってサーバーは受信したＩＤをもとに第１復号鍵８２５を検索することができる。こうして第１コンピュータから第２コンピュータ８２１ａへの暗号通信が成立する。この場合、第１暗号鍵と第１復号鍵は公開鍵暗号ではなく、共通鍵暗号の共通鍵ならば同じ鍵となる。

【００１９】利用者はディスク８０１の中に、例えば、１０００本収納されている暗号化されたコンテンツの１部、例えばコンテンツ番号８２６がｎのコンテンツを利用したい場合、コンテンツ番号８２６つまりｎを第１暗号鍵８１６である公開鍵を用いて、公開鍵暗号関数から構成される第１暗号エンコーダ８２７で、暗号化した暗号を第２コンピュータ８２１ａに送信する。第２コンピュータ８２１ａ側では前述のようにこの暗号を復号するための第１復号鍵８２５を検索し知っている。従ってこの暗号を確実に平文化できる。こうしてユーザーの発注情報のプライバシーは暗号により守られるという効果がある。

【００２０】この場合第１暗号鍵８１６として公開鍵暗号の秘密鍵を用いて署名してもよい。この方法は“デジタル署名”と呼ばれる。詳しい動作の説明は、暗号の専門書例えば、“Ｅ－Ｍａｉｌ　Ｓｅｃｕｒｉｔｙ　ｂｙ　Ｂｒｕｃｅ　Ｓｃｈｎｅｉｅｒ　１９９５”の“Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ”の項目等を参照されたい。

【００２１】暗号通信にもどるとこの暗号は通信部８２２とネットワーク８２３を介して、パスワード発行センター８２１の第１暗号デコーダ８２７に送られる。こうして、第１暗号鍵８１６と対になっている第１対暗号鍵８２５を用いて第１対暗号デコーダ８２７では、暗号が復号される。

【００２２】この場合、公開鍵は特定の１枚のディスクしかもっていないため、第３者のディスクからの不正な注文は排除できる。つまり、１枚のディスクの認証ができるためこのディスクの持ち主のユーザー個人の認証ができる。こうしてこのコンテンツ番号ｎは特定の個人の注文であることが証明されるため、第３者の不正な注文は排除できる。

【００２３】この時公開鍵８１６を秘密にしておけば、この手法でクレジットカード番号等の高いセキュリティが要求される課金情報の送信にも技術的には用いることができる。しかし、通常“モール”と呼ばれる店では、セキュリティの保証がないため、電子決済ではユーザーの課金情報は扱わない。クレジットカード系と銀行系の課金センター８２８のみが、ユーザーの金融情報を取り

扱うことができる。現在、ＳＥＴ等のセキュリティ規格の統一化が進められており、ＲＳＡ１０２４ｂｉｔの公開鍵暗号が使われ金融情報の暗号化が実現する可能性が高い。

【００２４】次に本発明の場合の課金情報の暗号通信手順を示す。まず、ＢＣＡ再生部８２０で再生された公開鍵暗号の第２暗号鍵８１７を用いて、個人のクレジットカード番号等の課金情報８３０は第２暗号エンコーダ８３１により、ＲＳＡ等の公開鍵系暗号により、暗号化され、通信部８２２より第２コンピュータ８２１を介して第３コンピュータ８２８の暗号デコーダ８３２に送られる。この場合デジタル署名をする場合は第２暗号鍵８１７は秘密鍵８２９を用いる。

【００２５】パスワード発行センター８２１の第２コンピュータ８２１ａの暗号鍵の場合の手順と同様にして暗号鍵データベースＤＢ８２４ａよりＩＤもしくは第２暗号鍵８１７に対応する第２復号鍵８２９を検索し、これを用いて第２暗号デコーダ８３２において暗号化された課金情報を復号することができる。

【００２６】なお第２暗号エンコーダ８３１で秘密鍵８２９を用いてデジタル署名すれば、第２暗号デコーダ８３２ではユーザーの署名を確認できる。こうして課金センター８２８は、ユーザーのクレジットカード番号や銀行カード番号や銀行パスワード等の課金情報をインターネットを使っても安全に入手することができる。インターネットのようなオープンなネットワークではセキュリティが問題となるが、このシステムでは、暗号通信用の暗号鍵（公開鍵）もしくはかつデジタル署名の秘密鍵がＢＣＡに記録されているので、暗号通信もしくは認証が確実に行える。このため不正な第３者による不正課金と不正注文を防げるという効果がある。またディスク毎つまりユーザー毎に異なる公開鍵を用いることができるので通信の秘密性が向上し、ユーザーの課金情報が第３者に漏洩する可能性が減少する。

【００２７】ここで、図６に戻り、パスワードの発行手順とパスワードによる解錠手順を説明する。パスワード発行センター８２１では、ＩＤとユーザーが解鍵したいコンテンツ番号とユーザーの使用許可期間を示す時間情報、の３つの情報に基づき、公開鍵暗号等の演算式を用いたパスワード生成部８３４でパスワードを生成し、第１コンピュータ９０９へ送信する。最も簡単な構成例を述べると、第２コンピュータではｎ番目のコンテンツの暗号を解除する復号鍵ディスクＩＤと時間情報を混合した情報を公開鍵暗号の公開鍵で暗号化し、これを解く秘密鍵を混合したｎ番目のパスワード８３４ａをパスワード生成部８３４で作成し、第１コンピュータ９０９へ送信する。第１コンピュータは上述のｎ番目のパスワードを受信し、秘密鍵でディスクＩＤと時間情報とｎ番目のコンテンツの復号鍵を復号する。ここで、ディスクより再生したＢＣＡのＩＤ８３５ａと現在の第２時間情報８３５ｂと許可されたＩＤ８３３ａと第１時間情報８３３を照合して一致するかをパスワード演算部８３６は演算する。もし一致すれば、許可し、ｎ番目の復号鍵８３６ａを暗号デコーダ８３７へ出力し、ｎ番目のコンテンツの暗号８３７ａが復号され、ｎ番目のコンテンツ８３８が出力される。出力される期間は第１時間情報８３３と第２時間情報８３５ｂが一致している間だけに制限される。第１コンピュータ９０９側では、ＩＤとパスワード８３５と現在の時間を示す時計８３６ｂからの時間情報の３つを情報をパスワード演算部８３６で演算し、ＩＤと時間情報が正しければ、正しい復号鍵が演算結果として出力されるので、ｎ番目の暗号が暗号デコーダ８３７で復号もしくは、デスクランブルされ、ｎ番目のコンテンツ８３８の平文データもしくは、デスクランブルされた映像信号もしくはオーディオ信号が出力される。

【００２８】この場合、時計８３６ｂの第２時間情報８３５ｂがパスワードの第１時間情報８３３と一致しないと暗号が正しく復号されないので再生はされない。時間情報を用いると、レンタル利用の際に３日間だけ映画を再生できるといった時間限定型のレンタルシステムに応用することが可能となる。

【００２９】図６ではブロック図を用いて手順を説明したが、この手順のフローチャートは図１６～図２３を用いて後で説明する。

【００３０】次に暗号鍵の容量についての工夫を述べる。こうして図７（ａ）に示すようにＢＣＡに第１暗号鍵８１６と第２暗号鍵８１７の双方を入れることにより、“モール”との商品取引と、“課金センター”との間の代金決済の２つのセキュリティが保たれるという効果が得られる。

【００３１】この場合、課金センターとのセキュリティに関してはＳＥＴ等の規格統一が予定されており、ＲＳＡ１０２４つまり、１２８ｂｙｔｅｓの暗号鍵が、第２暗号鍵領域８１７ａに収容されることになる。すると、ＢＣＡは１８８ｂｙｔｅｓしかないため、“モール”との取引の暗号鍵用には６０ｂｙｔｅｓしか残らない。２０バイトの大きさでＲＳＡ１０２４の１２８バイトと同程度のセキュリティをもつ暗号関数として楕円関数系公開鍵暗号が知られている。

【００３２】本発明では、第１暗号鍵領域８１６ａに楕円関数を用いている。楕円関数はＲＳＡ１０２４と同等のセキュリティが２０バイトで得られる。このため、楕円関数を用いることにより１８８バイトのＢＣＡ領域に、第１暗号鍵８１６と第２暗号鍵７１７の双方が収容できるという効果がある。

【００３３】以上述べたように、ＢＣＡを光ＲＯＭディスクに適用することにより、ディスク固有のＩＤ番号、第１と第２暗号鍵、接続のアドレスが記録できる。この場合インターネットを利用した場合に、自動的にモールに接続され、コンテンツの暗号解除による商品流通と、

商品購入の認証と秘密保持、代金決済時の認証と機密性の保持等のセキュリティがＢＣＡに暗号鍵が記録されたディスクを配布するだけで、実現する。このため本発明の暗号通信の方法により、従来のようなＩＤや、暗号鍵をユーザーへ配布するためにＩＣカードやフロッピィや手紙を用いるという作業がセキュリティを落とすことなしに省略でき合理化できるという大きな効果がある。またインターネットの接続アドレスであるＵＲＬは固定ではなく、変更される。原盤にはＵＲＬが記録されており、このＵＲＬに接続すればよいが、変更された時原盤を変更するのは、時間的コスト的に効率が悪い。ＢＣＡに変更されたＵＲＬを記録しておき、ＢＣＡより接続アドレス９３１が再生された場合のみ原盤の接続アドレスよりＢＣＡ接続アドレス９３１を優先して接続すれば、原盤を新規に作成することなく、変更された接続アドレス９３１に接続されるという効果がある。

【００３４】図６ではＢＣＡに公開鍵の第１号鍵と公開鍵の第１号鍵を記録した場合を示した。

【００３５】図８では、ＢＣＡに公開鍵の第１暗号鍵８１６と秘密鍵の第３復号鍵８１７ａの２つを記録した場合と暗号鍵を発生させて暗号通信する場合の２種類の実施例を示す。図６と同様の手順であるため、違う点のみを述べる。まず、プレス工場では、第１暗号鍵８１６と第３復号鍵８１７ａがＢＣＡに記録される。第３復号鍵８１７ａは課金センターからの公開鍵で暗号化された暗号の受信に用いる。この場合、受信のセキュリティが向上するという効果がある。

【００３６】まず、図８を用いて暗号鍵を生成するより具体的な暗号通信の例を説明する。第１暗号鍵８１６は公開鍵なので、受信用の第３復号鍵８１７ａをＢＣＡに記録する必要がある。一方ＢＣＡは容量が少ない。又公開鍵は処理時間を要する。そこで、図８では第１コンピュータ８３６で乱数発生器等で暗号鍵生成部８３８ａで公開鍵の暗号鍵／復号鍵の対、又は共通鍵を生成する。共通鍵の例を述べる。共通鍵Ｋ８３８を第１暗号鍵８１６と第１暗号エンコーダ８４２で暗号化し、第２コンピュータ８２１ａへ送る。第２コンピュータでは主復号鍵８４４を用いて、主暗号デコーダ８４３で、この暗号を平文化して共通鍵Ｋ８３８ａを得る。双方が共通鍵Ｋをもつので、第２暗号エンコーダ８４２ａと第２暗号デコーダ８４７ａに共通鍵Ｋを渡すことにより、店からユーザー、つまり第２コンピュータ８２１ａから第１コンピュータ８３６への暗号通信ができる。当然共通鍵Ｋを第２暗号エンコーダ８２７ａと第２暗号デコーダ８４５ａに渡すことにより、ユーザーから店つまり第１コンピュータ８３６から第２コンピュータ８２１ａへの暗号通信も可能となる。公開鍵である第１暗号鍵をＢＣＡに記録し、暗号鍵を生成する方式の効果を述べる。まず、第１暗号鍵の記録だけでよく復号鍵の記録が省略できる。従ってＢＣＡの少ない容量を減らすことがない。次にＢＣＡに復号鍵が記録されているので、セキュリティが向上する。共通鍵の場合、毎回鍵を変えればよい。

【００３７】演算時間が短いため、処理時間が少なくて済むという効果がある。この場合暗号鍵生成部８３８ａが共通鍵ではなく、公開鍵暗号の暗号鍵と復号鍵の一対を生成した場合暗号鍵を第２コンピュータ８２１ａへ暗号送信し、第２暗号エンコーダ８４２ａの暗号鍵として用い、復号鍵を第２暗号デコーダ８４７の復号鍵として用いれば処理時間は長くなるが共通鍵に比べてよりセキュリティを高めることができる。処理するＣＰＵの性能が高い場合は公開鍵を使う方が望ましい。公開鍵を新たに生成する場合は、ＢＣＡには第１暗号鍵の公開鍵しか記録されないため、セキュリティの問題発生しない。ＢＣＡの容量も消費されない。また暗号鍵を変更する必要がないためメンテナンスも容易となる。

【００３８】今度はパスワード発行センター８２１の第２コンピュータ８２１ａで共通鍵Ｋ８３８ａを定義した場合、共通鍵を第３暗号鍵８３９を用いて第３暗号エンコーダ８４０で暗号化し、パソコン８３６へ送信する。パソコン８３６側ではＢＣＡより再生した秘密鍵である第３復号鍵８３７を用いて、第３暗号デコーダ８４１で平文化することにより、共通鍵Ｋ８３８ｂを得る。この場合、秘密鍵である第３復号鍵８１７ａはこのユーザーしかもっていないので、センターからユーザーへの通信の内容が第３者に漏洩することは防止されるという効果がある。この場合のフォーマットを図７（ｂ）に示す。第３復号鍵８３９ｂは楕円関数を用いると２０バイトでよいためＢＣＡに収容できる。

【００３９】次に図９を用いて、暗号化ディスクにＢＣＡを用いて原盤作成費用を削減する実施例を説明する。

【００４０】ｎ個例えば、１０００本の平文のコンテンツ８５０があると、各々１～ｍ番目の暗号鍵８５１を用いて暗号エンコーダ８５２で暗号化する。この暗号化された第１～ｍ番目のコンテンツ８５３と１～ｍ番のコンテンツの復号プログラム８５４ａと第２暗号を復号するプログラムである第２暗号デコーダ８６１ａは、原盤に凹凸のピットとして記録された後、１枚の基板に成形され反射膜を形成した後、２枚の基板が貼り合わせられて、光ディスク８０１が完成する。この時、ディスク１枚目に異なるディスク固有の識別情報、いいかえるとＩＤ８５５とｎ番目、例えば１番目のコンテンツを解錠するパスワードや復号鍵等の復号情報８５４を第２暗号エンコーダ８６０で暗号化した第２暗号を予めＢＣＡに記録する。すると、再生装置ではＢＣＡ再生部８２０より第２暗号が再生される。ＢＣＡ以外の通常の記録データが再生されるデータ再生部８６２よりは第２暗号デコーダ８６１が再生されるので、これを用いて第２暗号を復号し、ＩＤ８５５ａと第ｎ番目のパスワード８５４ａが再生される。暗号デコーダ８５５ｂでは、データ再生部８６２より再生したｎ番目のコンテンツの復号プログラ

ム８５４ａを用いて、ＩＤ８５５ａとパスワード８５４ａを用いて第１暗号を復号し、ｎ番目のコンテンツの平文８５５ｃと識別情報８５５ａを得る。パソコンの場合はハードディスク８６３にコンテンツとＩＤは記録される。このＩＤ８５５ａは、プログラム起動時にネットワーク上に同じＩＤがないかをチェックし、ネットワークプロテクションを動作させるので、ソフトの不正インストールが防止できるという副次的効果がある。つまり、原盤１枚に暗号化した１千本のコンテンツを入れ、特定のソフトに対応するパスワード等の復号情報を記録しておけば、実質的に特定の１本のコンテンツの光ＲＯＭディスクを作成したのと等価となる。１枚の原盤で１０００種類のソフトの原盤をカッティングしたのと同じ効果が得られ、原盤作成費用と手間が削減できるという効果がある。

【００４１】図１０ではＲＡＭディスクに、コンテンツを記録する際にＢＣＡを用いて暗号化する手順を述べる。まず、ＲＡＭディスク８５６よりＢＣＡ再生部８２０により、ＢＣＡのデータを再生し、ＩＤ８５７を出力し、インターフェース８５８ａ，８５８ｂとネットワークを介して、暗号化部８５９に送る。暗号化部８５９ではコンテンツ８６０をＩＤ８５７を含む鍵で暗号エンコーダ８６１において暗号化もしくは映像音声信号のスクランブルを行う。暗号化されたコンテンツは記録再生装置に送られ記録回路８６２によりＲＡＭディスク８５６に記録される。

【００４２】次に、この信号を再生する時は、データ再生部８６５により、主データの復調を行い、暗号化された信号を再生し、暗号デコーダ８６３において、復号が行なわれる。この時、ＲＡＭディスク８５６のＢＣＡ領域から、ＢＣＡ再生部８２０により、ＩＤ８５７を含む情報が再生され、暗号デコーダ８６３に鍵の一部として送られる。この時、正規にコピーされた場合はＲＡＭディスクに記録された暗号の鍵は正規のディスクＩＤであり、ＲＡＭディスクのＩＤも正規のディスクＩＤであるため、暗号の復号もしくはデスクランブルが行なわれ、第ｎ番目のコンテンツの平文８６４が出力される。映像情報の場合はＭＰＥＧ信号が伸長されて、映像信号が得られる。

【００４３】この場合、暗号化はディスクＩＤを鍵としている。ディスクＩＤは世の中に１枚しか存在しないため、１枚のＲＡＭディスクにしかコピーできないという効果が得られる。

【００４４】ここで、もしこの正規のＲＡＭディスクから、別のＲＡＭディスクにコピーした場合、最初の正規ディスクＩＤであるＩＤ１と、別の不正のＲＡＭディスクのディスクＩＤであるＩＤ２とは異なる。不正のＲＡＭディスクのＢＣＡを再生するとＩＤ２が再生される。しかし、コンテンツはＩＤ１で暗号化されているので、暗号デコーダ８６３においてＩＤ２で解鍵しようとしても、鍵が異なるため、暗号は復号されない。こうして、不正コピーのＲＡＭディスクの信号が出力されず、著作権が保護されるという効果がある。本発明はＤｉｓｋＩＤ方式なので正規に１回だけコピーされた正規のＲＡＭディスクはどのドライブで再生しても、暗号が解錠されるという効果がある。ただし、暗号化部８５９はセンターのかわりに暗号エンコーダを搭載したＩＣカードでもよい。

【００４５】図１１のブロック図と図１２のフローチャートを用いて、コピー防止方法を述べる。ステップ８７７ａでインストールプログラムを動作させる。ステップ８７７ｂで貼り合わせた光ディスク８０１より、ＢＣＡ再生部８２０より副情報のＩＤが出力される。ステップ８７７ｄでデータ再生部８６５より主情報よりコンテンツとネットワークチェックソフト８７０が再生される。コンテンツとＩＤ８５７はＨＤＤ８７２に記録される。ステップ８７７ｃで不正に改ざんされないようＩＤ８５７は特定の秘密の暗号演算を行い、ＨＤＤ８５７にソフトＩＤとして記録される。こうして、パソコン８７６のＨＤＤ８７２にはコンテンツとともにソフトＩＤ８７３が記録される。ここで図１２のステップ８７７ｆのプログラムを起動する場合を述べる。プログラムを起動する時は、ステップ８７７ｇにおいて、ＨＤＤ８７２のソフトＩＤ８７３を再生し、インターフェース８７５を介して、ネットワーク８７６の上の別のパソコン８７６ａのＨＤＤ８７２ａの中のソフトＩＤ８７３ａをチェックする。ステップ８７７ｈで他のパソコンのソフトＩＤ８７３ａと自分のソフトＩＤ８７３が同一番号であるかをチェックし、同一番号である場合は、ステップ８７７ｊへ進み、パソコン８７６のプログラムの起動を中止するか画面上に警告メッセージを表示する。

【００４６】他のパソコンのソフトＩＤ８７３ａが同一番号でなかった場合は、少なくともネットワーク上にはコンテンツを複数台にインストールした形跡はないため不正コピーはないと判断し、ステップ８７７ｋへ進み、プログラムの起動を許可する。この場合、他のパソコンへネットワークを介してソフトＩＤ８７３を送信してもよい。このパソコンでは各パソコンのソフトＩＤの重複をチェックすれば不正インストールが検出できる。不正があれば、該当するパソコンに警告メッセージを送る。

【００４７】こうして、ＢＣＡにＩＤを記録し、ネットワークチェックプログラムをピット記録領域に記録することにより、同一ネットワーク上の同一ＩＤのソフトの複数インストールを防止できる。こうして簡便な不正コピープロテクトが実現する。

【００４８】図１３のように白色の材料からなる書き込み可能な書き込み層８５０を塗布することにより設けることにより、文字を印刷したりペンでパスワード等を書き入れることができるだけでなく、書き込み層８５０が厚くなるため光ディスクの基板の損傷を防ぐという効果

も得られる。この書き込み層８５０の上のＢＣＡ領域８０１ａにトリミングで記録されたＢＣＡデータ８４９の一部であるディスクＩＤ８１５を平文化し英数字に変換した文字８５１と一般バーコード８５２を印字することにより、販売店やユーザーがＢＣＡを再生装置でよみとることなく、ＰＯＳのバーコードリーダーや視認でＩＤの確認や照合ができる。視認できるＩＤはユーザーがパソコン経由でＩＤをセンターに通知する場合は不要である。しかしユーザーが電話でＩＤをセンターに口頭で伝える場合は、ＢＣＡのＩＤと同じＩＤがディスク上に視認できる形式で印刷することにより、ユーザーがＩＤを目でよみとれるのでパソコンにディスクを挿入することなしにＩＤをセンターに伝えることができる。図１３のフローチャートで光ディスクの製造ステップを説明する。ステップ８５３ｄで、原盤よりディスクの成形を行い、ピットの記録された基板を作成する。ステップ８５３ｅでアルミ反射膜を作成する。ステップ８５３ｆで２枚のディスク基板を接着剤で貼り合わせ、ＤＶＤディスク等を完成させる。ステップ８５３ｇでスクリーン印刷のラベル印刷をディスクの片面に行う。この時バーコードで原盤に個有の識別情報を記録する。ステップ８５３ｈでＰＯＳ用バーコードのフォーマットでディスク１枚ごとに異なるＩＤ等の識別情報をインクジェットバーコード印刷機や熱転写型バーコード印刷機で印刷する。ステップ８５３ｉで、このバーコードをバーコードリーダーでよみ出し、ステップ８５３ｊで識別情報に対応したＢＣＡデータをディスクの第２記録領域に印刷する。この製造方法であると、ＢＣＡを除くＰＯＳバーコードを含む全工程を終えた後にディスク識別情報を確認した上で、ＢＣＡデータを記録する。ＢＣＡはディスクを再生しないと読めないが、ＰＯＳバーコードは密度が低いので市販のバーコードリーダーでよみとれる。工場の中のあらゆる工程で、ディスクＩＤが識別できる。ＢＣＡトリミングの前にＰＯＳバーコードでディスクＩＤを記録しておくことにより、ＢＣＡとＰＯＳバーコードの誤記録がほぼ完全に防止できる。

【００４９】このＢＣＡ方式で二次、三次記録もできるＢＣＡの利用方法について述べる。図１５に示すようにソフトメーカでは、工程（２）で示すように海賊版防止マークと照合暗号を二次記録もできる。工程（２）ではディスク１枚ごとに異なるＩＤ番号やユーザーとの秘密通信用の暗号鍵を記録したディスク９４４ｂを作成しても良い。このディスク９４４ｃ、９４４ｄはパスワードを入力しなくても再生できる。

【００５０】別の応用として工程（３）では、暗号化やスクランブルしたＭＰＥＧ映像信号等の情報をディスク９４４ｅに記録する。ＭＰＥＧスクランブルの詳しい動作は説明を省略する。ソフト会社では工程（４）においてＩＤ番号とスクランブル解除情報を復号するためのサブ公開鍵をＢＣＡで二次記録したディスク８４４ｆを作成する。このディスクは単独では再生はできない。工程（５）では、販売店でディスクの代金を受け取った後にサブ公開鍵とペアになっているサブ秘密鍵でパスワードを作成し、ディスクに三次記録する。もしくはパスワードの印刷されたレシートをユーザーに渡す。このあと、ディスク８４４ｇはパスワードが記録されているためユーザーが再生可能となる。この方式を用いると、代金の支払われていないディスクを万引きしても映像のスクランブルが解除されないため正常に再生されないため、万引きが無意味になり減るという効果がある。

【００５１】レンタルビデオ等の店では恒久的にパスワードをＢＣＡ記録すると万引きされた場合、使用されてしまう。この場合は工程（６）に示すように店でＢＣＡをＰＯＳバーコードリーダーでよみとりスクランブル解除のためのパスワードをステップ９５１ｇで発行し、ステップ９５１ｉでレシートに印刷し、ステップ９５１ｊで客に手渡す。客の方は、自宅でステップ９５１ｋでレシートのパスワードをプレーヤにテンキーで入力する。ステップ９５１ｐで所定の日の間だけ再生される。ディスクの一部のソフトのパスワードのみを与えてレンタルした場合に、他のソフトをみたい時は、電話で、そのソフトのパスワードをステップ９５１ｕで通知しステップ９５１ｋで入力することにより、ディスクの他のソフトを再生することができる。レンタルビデオ店の例を示したがパソコンソフト店で、暗号化したパソコンソフトを売った時に、ＰＯＳ端末でパスワードを印刷して渡しても良い。

【００５２】図１５の工程（５）（６）のセル販売店、レンタル店における動作を図１４を用いてより具体的に説明する。セル販売店ではソフトメーカーから暗号やスクランブルがかかったディスク９４４ｆを受け取り、ユーザーからの入金を確認するとバーコード記録装置９４５よりディスク９４４ｆのＩＤ番号、サブ公開鍵のデータをＰＯＳ端末９４６経由でパスワード発行センター９５２に送信する。小規模なシステムの場合パスワード発行センター、つまりサブ公開鍵のサブ秘密鍵を含むシステムはＰＯＳ端末の中にあっても良い。パスワード発行センターはステップ９５１ｑでディスクＩＤ番号と時間情報を入力し、ステップ９５１ｓで演算を行い、ステップ９５１ｔで、サブ秘密鍵を用いて暗号化し、ステップ９５１ｇでパスワードを発行しネットワーク９４８とＰＯＳ端末８４６を介してＢＣＡバーコード記録装置９４５にパスワードを送り、記録されたディスク９４４ｇが客に渡される。このディスク９４４ｇは、そのまま再生できる。

【００５３】次にレンタル店やパソコンソフト店の場合、まず暗号やスクランブルの解除されていないＲＯＭディスク９４４ｆを店頭に陳列する。客が特定のＲＯＭディスク９４４ｆを指定した場合、うずまき型にスキャンする回転型の光学ヘッド９５３を内蔵した円形バーコ

ードリーダ９５０を手に持ち透明ケース入りのディスク９００の中心におしつけることにより、ディスク９４４ｆの無反射部９１５による反射層のバーコードを読み取り、ディスクＩＤ番号を読み取る。ディスクＩＤの商品バーコードを図１３の８５２のように印刷することにより通常のＰＯＳ端末のバーコードリーダーで読み取ることが出来る。原盤に予め記録されプレスされた円形バーコードから読み取っても良い。これらのディスクＩＤを含む情報はＰＯＳ端末９４６により処理され、料金がクレジットカードから決済されるとともに、前述のようにＩＤ番号に対応したパスワードがステップ９５１ｇにおいてパスワード発行センターから発行される。レンタル用途の場合、視聴可能な日数を制限するためステップ９５１ｒで用いたように日付情報を加えて、ディスクＩＤ番号を暗号化しパスワードを作成する。このパスワードの場合、特定の日付しか作動しないため、例えば３日間の貸し出し期間をパスワードの中に設定できるという効果がある。

【００５４】さて、こうして発行されたデスクランブルのためのパスワードはステップ９５１ｉにおいて、貸出日、返却日、レンタルのタイトル料金とともにレシート９４９に印刷され客にディスクとともに渡される。客はディスク９４４ｊとレシート９４９を持ち帰り、ステップ９５１ｋでパスワードを図６の第１コンピュータ９０９のテンキー入力部９５４に入力することによりパスワード８３５はＩＤ番号８３５ａと演算されて暗号デコーダ８３７に入力され、復号鍵を用いて平分化される。正しいパスワードである場合のみ暗号デコーダ８３７でプログラムのデータをデスクランブルし、映像出力を出力させる。

【００５５】この場合、パスワードに時間情報が含まれている場合、時計部８３６ｂの日付データと照合し、一致した日付の期間、デスクランブルをする。なお、この入力したパスワードは対応するＩＤ番号とともにメモリ７５５の不揮発メモリ７５５ａにストアされ、ユーザーは一度パスワードを入力すると２度と入力することなしにデスクランブルされる。こうして流通において電子的にディスクの鍵の開閉ができるという効果がある。

【００５６】図１６を用いてソフトが暗号データとして記録されたディスクのソフトの復号方法を詳しく説明する。

【００５７】ステップ８６５は暗号データと個別ＩＤのユーザーへの配布の全体フローを示す。まず、ステップ８６５ａでは、１枚の原盤のＲＯＭ領域に、秘密の第１暗号鍵で暗号化されたｍヶのデータと、暗号化されたｍヶのデータを復号するプログラムを記録する。ステップ８６５ｂでは、原盤より基板を成形し、反射膜を付加した２枚の基板を貼り合わせて完成ＲＯＭディスクを複数枚、作成する。ステップ８６５ｃでは、完成ディスクの書換できない副記録領域（ＢＣＡとよぶ）に、暗号化データの復号に必要な復号情報（プレスしたディスク毎に異なるディスク識別情報　ａｎｄ／ｏｒ　暗号データの復号鍵）をＲＯＭ領域と異なる変調方法で記録する。ステップ８６５ｄでは、ユーザーは配布されたディスクを再生し、希望する暗号化データｎを選択し、復号処理を始める。ステップ８６５ｅで、ユーザーの第１コンピュータで、ＲＯＭ領域から暗号化データと復号プログラムを再生し、副記録領域（ＢＣＡ）から、復号情報を読み出す。ステップ８６５ｆで、オンラインで第２復号情報を得ない場合は図１７のステップ８７１ａで、ＩＤ等の復号の補助情報を画面上に表示する。ステップ８７１ｂで、ユーザーはＩＤに対応するパスワード等の第２復号を入手し、第１コンピュータに入力する。ステップ８７１ｃで、ディスク識別情報と第２復号情報と暗号化データｎを用いて公開鍵系暗号関数の特定の演算を行う。ステップ８７１ｄで結果が正しければ、ステップ８７１ｆでｎ番目のデータが平文化され、ユーザーはデータｎのソフトを動作させることができる。

【００５８】次に図１８のフローチャートを用いて、ＢＣＡを用いたインターネット等で必須な暗号通信の方法を述べる。ステップ８６８は、ユーザーへ通信プログラムと通信暗号鍵を配布する方法のルーチンである。まず、ステップ８６８ａで、１枚の原盤のＲＯＭ領域に少なくとも通信プログラムや接続情報を記録する。ステップ８６８ｂで、原盤より基板を成形し、２枚の基板を貼り合わせて完成ＲＯＭディスクを複数枚作成する。ステップ８６８ｃで、完成ディスクの書換できない副記録領域（ＢＣＡ）に、プレスしたディスク毎に異なるディスク識別情報と暗号通信用暗号鍵を記録する。場合により第２コンピュータの接続アドレス、もしくは／かつ暗号通信用復号鍵をＲＯＭ領域と異なる変調方法で記録する。ステップ８６８ｄで、ユーザーの第１コンピュータで、ＲＯＭ領域から通信プログラムと暗号化プログラムを再生し、副記録領域から、ディスク識別情報と通信用暗号鍵を読み出す。図１９に進みステップ８６７ａで、ＢＣＡ領域に接続アドレスがある場合は、ステップ８６７ｂで、ＢＣＡ領域のＵＲＬ等の接続アドレスに基づき第２コンピュータに接続し、接続アドレスがない場合はステップ８６７ｃのＲＯＭ領域の接続アドレスのコンピュータに接続する。ステップ８６７ｄで、送信データが入力され、ステップ８６７ｅで、ＢＣＡ領域に暗号通信用暗号鍵がある場合はステップ８６７ｇでＢＣＡ領域の暗号通信用暗号鍵を用いて、送信データを暗号化し、第３暗号を作成する。また、ない場合はステップ８６７ｆでＲＯＭ領域又はＨＤＤの暗号通信用の暗号鍵を用いてデータを暗号化し、第３暗号を作成する。

【００５９】次に図２０では第２コンピュータ９１０から受信した暗号の復号鍵の生成ルーチンをステップ８６９で述べる。まず、第１コンピュータではステップ８６９ａで、通信復号鍵が必要な場合は、ステップ８６９ｂ

へ進み、ＢＣＡに通信用復号鍵があるかどうかをチェックし、復号鍵がない場合は、ステップ８６９ｃでＲＯＭ領域から再生した暗号鍵／復号鍵の生成プログラムを用いてユーザーのキー入力もしくは乱数発生器のデータをＲＯＭ領域から再生した第２暗号器により一対の第２通信暗号鍵／第２通信復号鍵を新たに生成する。ステップ８６９ｄで、“第２通信暗号鍵もしくは／かつユーザーデータ”をＢＣＡに記録された通信暗号鍵とＲＯＭ領域から再生して得た暗号化ソフトを用いて暗号化した第４暗号を作成する。ステップ８６９ｅで、第４暗号と、ディスク識別情報もしくは／かつユーザーアドレスを、ディスクから再生して得た接続アドレスの第２コンピュータに送信する。第２コンピュータの処理としては、ステップ８６９ｆで、第４暗号とディスク識別情報とユーザーアドレスを受信する。ステップ８６９ｇでは、復号鍵データベースから、ディスク識別情報と対になった通信復号鍵を選択し、これを用いて第４暗号を復号し、第２通信暗号鍵の平文を得る。ステップ８６９ｈで、第２通信暗号鍵を用いて、ユーザーデータの一部を含むサーバーのデータを暗号化した第５暗号を第１コンピュータへインターネット９０８で送信する。ステップ８６９ｉで、第５暗号（とディスク識別情報）を受信し前述の第２通信復号鍵とＲＯＭ領域に記録された復号関数を用いて復号し、前述のサーバーデータの平文を得る。こうして、図２０のステップ８６９の方式で、第１、第２コンピュータ間で双方向の暗号通信が実現する。

【００６０】図２１のステップ８７０では課金情報の受信ルーチンについて説明する。ステップ８７０ａで、課金情報を入力する場合は、課金通信用の公開鍵暗号の第３暗号鍵を第２コンピュータへ要求する。ステップ８７０ｂでは、第２コンピュータが、第３コンピュータへ第３暗号鍵を要求する。やりとりのステップは省略するが、第３コンピュータ９１１はＩＤと第３暗号鍵を第２コンピュータ９１０へ送信する。ステップ８７０ｃで、第２コンピュータはＩＤと第３暗号鍵を受信し、ステップ８７０ｅで、第３暗号鍵を第２通信暗号鍵等を用いて暗号化した第７暗号を第１コンピュータへ送信する。第１コンピュータではステップ８７０ｆで、第７暗号を受信し、ステップ８７０ｇで、前述の第２通信復号鍵を用いて、受信した第７暗号を復号し、第３暗号鍵（公開鍵関数の公開鍵）を得る。ステップ８７０ｈでは、必要に応じて第３暗号鍵をＨＤＤに記録する。これは次回の送信時に利用する。ステップ８７０ｉで、クレジットカード番号や決済用パスワード等の機密値が高い課金情報を入力する場合は、ステップ８７０ｊで第３暗号鍵を用いて、上記課金情報を暗号化した第８暗号を第２コンピュータ経由で第３コンピュータへ送る。第２コンピュータは、ステップ８７０ｋで第８暗号を受信し、第３コンピュータへ再転送する。第３暗号の復号鍵は金融機関である第３コンピュータ９１２しか持っていないため、第２コンピュータの電子商店では解読できない。第３コンピュータではステップ８７０ｍで、暗号鍵データベースからディスク等の識別情報を用いて第３暗号鍵に対応した第３復号鍵を探しだし、公開鍵暗号の秘密鍵である第３復号鍵で第８暗号を復号し、課金情報の平文を得る。ステップ８７０ｎでは、ユーザーの信用情報や預金残高等の金融情報から、代金が回収できるかをチェックし、ステップ８７０ｐでは、調査結果を第２コンピュータへ通知する。第２コンピュータいわゆる電子商店はステップ８７０ｑで代金の回収可能かどうかを判定して、不能と判断すれば、ステップ８７０ｒで、商品の発送や暗号ソフトを復号する鍵の送付をしない。代金回収可能と判断した場合、図１６のような鍵提供システムの場合、ステップ８７０ｓへ進み、暗号ソフトの復号鍵つまり商品をインターネット９０８で、ユーザーの第２コンピュータに送信する。第１コンピュータでは、ステップ８７０ｔで、暗号ソフトの復号鍵を受信して、ステップ８７０ｕでｎ番目の暗号化ソフトの暗号を解除して、ステップ８７０ｗで、ソフトの平文を得る。こうして、コンテンツの鍵提供システムが実現する。

【００６１】この図２１のステップ８７０の方式は課金情報という高いセキュリティが要求される第３暗号鍵の公開鍵を第３コンピュータつまり、金融機関に、必要に応じて要求し発行させる。ＢＣＡに予め記録しておかなくてもよい。従って第３暗号鍵にＲＳＡ２０４８の２５６バイトのさらに強力なＲＳＡ系の暗号鍵をＢＣＡの容量を消費することなしに用いることができるという効果がある。さらに全てのディスクのＢＣＡに予め記録する必要がないので、第３暗号鍵の発行総数が少なくなり、第３暗号鍵の演算に要するコンピュータのＣＰＵタイムが減る。また、第３暗号がＢＣＡにないため、公開されないため、セキュリティが若干向上する。この場合のＢＣＡの役割は、第１９、２０図のように、ＲＳＡ１０２４グレードの暗号鍵による秘密通信ディスクの識別情報の記録である。ＢＣＡディスク１枚あれば、第２コンピュータとの暗号通信が実現するため効果は高い。

【００６２】次に図２２を用いて、ＢＣＡに通信暗号鍵と通信復号鍵の双方を記録した時の、暗号通信のステップ８７２を説明する。ステップ８７２ｇで、第１コンピュータ９０９ではＢＣＡから再生して得た通信暗号鍵でユーザーデータを暗号化した第９暗号と、原盤作成時にＲＯＭ領域に記録された基本識別情報と、ＢＣＡ領域に記録されたディスク識別情報を第２コンピュータ９１０へ送信する。第２コンピュータでは、ステップ８７２ｂで、第９暗号とディスク識別情報と基本識別情報を受信する。ステップ８７２ｃで、復号鍵データベースからディスク識別情報と対になった通信復号鍵を検索し、第９暗号を復号し、ユーザーデータの平文を得る。ステップ８７２ｅで、ディスク識別情報に対応した第２暗号鍵を暗号鍵データベースから選別し、この第２暗号でサーバ

ーデータと図２１で述べた手順で第３コンピュータから受信した第３暗号鍵を暗号化した第１０暗号を第１コンピュータへ送信する。第１コンピュータではステップ８７２ｆで、第１０暗号を受信し、ステップ８７２ｇで、ＢＣＡに記録された前述の通信用第２復号鍵を用いて、受信した第７暗号を復号し、サーバーデータと第３暗号鍵（公開鍵関数の公開鍵）の平文を得る。ステップ８７２ｈで必要に応じて第３暗号鍵をＨＤＤに記録する。ステップ８７２ｉで課金情報を入力する場合は、ステップ８７２ｊへ進み、第３暗号鍵を用いて、上記課金情報を暗号化した第８暗号と第１暗号を第２コンピュータ経由で第３コンピュータへ送る。第２コンピュータでは、ステップ８７２ｍで、第１１暗号を第３コンピュータへ再送信する。第３コンピュータでは、ステップ８７２ｍで、第３暗号鍵をデータベースからディスク等の識別情報と対になった第３暗号鍵を探しだし、第８暗号を復号し、課金情報の平文を得る。ステップ８７２ｎでは、ユーザーへの課金回収の可能性のチェックを行い、ステップ８７２ｐで調査結果を第２コンピュータへ送信する。第２コンピュータではステップ８７２ｑでユーザーが課金の回収が可能かどうかをチェックする。代金回収可能と判断した場合図１６のような鍵提供システムの場合、ステップ８７２ｓへ進み、暗号ソフトの復号鍵、つまり商品をインターネットでユーザーの第２コンピュータに送信する。第１コンピュータではステップ８７２ｔで暗号ソフトの復号鍵を受信して、ステップ８７２ｕでｎ番目の暗号化ソフトの暗号を解除してステップ８７２ｗでソフトの平文を得る。こうして、コンテンツの鍵提供システムが実現する。

【００６３】図２２のステップ８７２の方式の効果の特長は、暗号鍵と復号鍵の双方がＢＣＡ領域に記録されているため、第２コンピュータからの受信に必要な復号鍵や暗号鍵の送信が必要ないという点である。ＢＣＡの容量は最大１８８バイトであるので、公開鍵等の暗号関数なら、ＲＳＡ５１２バイトで６４バイト２ヶで、１２８バイトで済むので記録できる。ＲＳＡ５１２にグレードの双方向の暗号化が可能となる。楕円関数なら図７に示したように７～８ヶ収容できるため、効果はさらに高い。

【００６４】図２３を用いて、ＢＣＡに第１暗号鍵と第３暗号鍵を予め記録した場合の動作と効果について述べる。なお、図２２のステップ８７２ａ～８７２ｗと図２３のステップ８７３ａ～８７３ｗは、ほぼ同じ構成なので違うステップだけを説明する。

【００６５】まず、課金情報等の金融情報のセキュリティを守る第３暗号鍵がＢＣＡに記録されているので、ステップ８７３ｅにおいて第２、第３コンピュータは第３暗号鍵の生成と送信は不要となる。ステップ８７３ｅ、８７３ｆ、８７３ｇにおいて第１２暗号の送受信が行われる。また、ステップ８７３ｊにおいてはＢＣＡ領域から第３暗号鍵を読み出し、ユーザーの課金情報を第２コンピュータ経由で第３コンピュータへ送る。図２３の方法は、第３暗号鍵の生成、送受信が全く不要となるため、手順が簡単になるという効果がある。

【００６６】さて、電子決済システムの場合、課金センターはクレジット開始と同様、通常、複数個存在する。従って、当然公開鍵である第３暗号鍵は複数個必要となる。図７（ｂ）で説明したようにＲＳＡ暗号関数を使うとＲＳＡ１０２４グレート以上つまり１２８バイト以上必要であるので、ＢＣＡの１８８バイトには１ヶしか第３暗号鍵８１７ｂは入らない。しかし、近年登場した楕円関数系暗号鍵（楕円暗号）は小容量でＲＳＡと同等のセキュリティが得られる。近年ではＲＳＡ関数のＲＳＡ１０２４が金融情報のセキュリティの最低基準となっている。ＲＳＡ関数だと１２８バイト必要であるが、同等のセキュリティを得るのに、楕円暗号であると、２０～２２バイト程度で良いといわれている。従って図７（ｃ）に図示するように金融情報を取り扱う第３暗号を複数ヶ、最大７～８つＢＣＡに収容できる。楕円暗号を使うことにより、現実的に必須である複数の金融センターに対応した、ＢＣＡ応用の電子決済システムが実現する。第３暗号に的を絞って説明したが、第１暗号鍵の公開鍵に用いても、複数の電子商店との間の高いセキュリティが保たれるため楕円暗号の効果は同様である。

【００６７】次に図２４を用いて、図１０で説明したＢＣＡを用いたＲＡＭディスク記録再生装置に関して更に詳しく述べる。１つの実施例としていわゆるＰａｙ ｐｅｒＶｉｅｗシステムにおけるＲＡＭディスクへの記録手順を述べる。まず、ＣＡＴＶ会社等のソフト会社は番組送信器８８３において、映画ソフト等のコンテンツ８８０を第１暗号鍵８８２を用いて第１暗号器において暗号化し、第１暗号９００を生成し、各ユーザーのＣＡＴＶデコーダの如きデコーダ８８６に送信する。デコーダ８８６側ではネットワークを介して鍵発行センター８８４へ特定の番組の要求を送ると、鍵発行センター８８４は、特定のソフトでかつ特定のデコーダのシステムＩＤ番号かつ特定の時間制限情報９０３に対するスクランブル解除キーの如き第１復号情報でかつ、ＲＡＭディスクへの記録許可カード９０１が含まれている第１復号情報８８５ａを第１デコーダ８８６の第１復号部８８７へ送信する。第１復号部８８７はシステムＩＤ８８８と第１復号情報８８５ａより、第１暗号９００を復号し、映像信号の場合は、一旦デスクランブルされた信号がさらに別の暗号でコピー防止用のスクランブルされた信号が第３暗号出力部８８９から出力され、一般ＴＶ８９９で、元のＴＶ信号がコピーガードされているが視聴できる。ここで、記録許可コード９０１ａがＮＯの場合は、ＲＡＭディスク８９４に記録できない。しかし、ＯＫの場合はＲＡＭディスク８９４の１枚に限り記録できる。この方法を説明する。

【００６８】デコーダ８８６では、ＩＣカード９０２が挿入され、ＲＡＭレコーダのＲＡＭディスク８９４のＢＣＡをＢＣＡ再生部８９５が読み取りディスクＩＤ９０５がＩＣカード９０２に送られる。ＩＣカード９０２はディスクＩＣ９０５とデコーダ８８６から得た現在の時間情報９０４と記録許可コード９０１ａをチェックし、第３暗号出力部８８９と双方向でシェイクハンド方式のコピーチェック９０７を行い、記録許可コードとコピーチェックがＯＫならＩＣカード９０２の中の第２副暗号器８９１は第２暗号鍵９０６を発行する。第２暗号器８９０において、第３暗号は再暗号化されて特定の１枚のディスクのディスクＩＤでコンテンツ８８０が暗号化された第２暗号が生成され、ＲＡＭレコーダ８９２に送られ記録手段８９３において８－１５や８－１６変調を用い、第１変調部により変調され、レーザにより、ＲＡＭディスク８９４の第１記録領域８９４ａに第２暗号９１２が記録される。こうしてＲＡＭディスク８９４のデータは特定のディスクＩＤの番号で暗号化される。

【００６９】次にこのディスクを通常の再生手段８９６で再生信号を８－１６変調の第１復調部８９６ａで復調するとコンテンツの第２暗号が出力される。第２復号器８９７は複数の第２復号鍵８９８ａ、８９８ｂ、８９８ｃをもつ。これは各ＣＡＴＶ局等の番組供給会社毎に異なる各々のＩＣカードの暗号鍵に対応した復号鍵をもつことになる。この場合、デコーダ８８６もしくはＩＣカード９０２の復号鍵識別情報は記録時に第１記録領域８９４ａに記録されている。再生装置では、第１記録領域８９４ａから復号鍵識別情報９１３をよみ出し、復号鍵選別手段９１４により復号鍵８９８ａ～８９８ｚのうちからを元に各々の暗号鍵に対応した、第２復号鍵８９８ａを自動的に選択し、ディスクＩＤ９０５ａを一つの鍵として、第２暗号は第２復号器８９７において復号される。特定の復号鍵の入ったＩＣカードを用いてもよい。映像の場合ＴＶ８９９ａにてデスクランブルされた正常な映像が得られる。

【００７０】図２４のシステムでは、各ユーザーの自宅のデコーダに挿入したＩＣカードにディスクＩＤ９０５を送り、画像データ等を暗号化するので、ソフト会社８８３は各ユーザーに配信するコンテンツの暗号を個別に変える必要がない。従って、衛星放送やＣＡＴＶのように大量の視聴者にペイパービューのスクランブル映像を放送する場合に、各ユーザー毎にＲＡＭディスク１枚だけに記録することを許可することができるという効果がある。

【００７１】図２４のシステムで１枚のディスクに記録すると同時に、２枚目つまり他のディスクＩＤのＲＡＭディスクに不正にコピーつまり記録しようとするとＢＣＡの場合２層ディスクを用いているのでディスクＩＤを改ざんすることができないため、同時間に２枚目のディスクへの不正コピーは防止される。次に別の時間帯に擬似的な記録許可コード９０１ａや第３暗号をデコーダやＩＣカードに送信し、特定のディスクＩＤでデータは暗号化されている。別のディスクＩＤのＲＡＭディスクに記録することが考えられる。こうした不正行為にも、ＩＣカードの中のデコーダ時間情報管理部９０２が鍵発行センター８８４の時間制限情報９０３やコンテンツの時間情報の時間とデコーダの中の時間情報部９０４ａの現在の時間とを比較して、時間が一致しているかどうかをチェックし、ＯＫならＩＣカード９０２は第２暗号演算器９９０の暗号化を許可する。

【００７２】この場合、第２暗号器８９０と第１復号部８８７が双方向でチェックデータを交信するシェイクハンド方式の時間チェック方式でもよい。

【００７３】シェイクハンド方式の場合、ＩＣカードを含む第２暗号演算器８９０と、第１復号部８８７と第３暗号部８８９は双方向で、暗号データを確認しあう。このためコンテンツの送信時間と同一でない別の時間帯の不正コピーは防止される。

【００７４】こうして各ユーザーのもつデコーダ８８６においては世の中に１枚しか存在しない特定のディスクＩＤのＲＡＭディスク８９４の１枚のみに、ソフト会社のコンテンツが記録される。そして、このディスクはどのＲＡＭディスク再生機でも再生できる。図２４の方式でＲＡＭディスクに記録する場合でもソフト会社の著作権が守られるという効果がある。

【００７５】なお本文の図の説明では、暗号エンコーダで暗号化、暗号デコーダで復号化を説明したが、実際はＣＰＵの中のプログラムである暗号アルゴリズム及び復号アルゴリズムを用いる。

【００７６】

【発明の効果】このように、光ディスクのＢＣＡ領域にＩＤや暗号の暗号鍵や復号鍵を予め記録しておくことにより、暗号化されたコンテンツの暗号解除がより簡単な手順で実現する。また通信の機密性が従来の登録手続きなしで実現する。ネットワークチェックプログラムをコンテンツに収納しておくことにより、同一ネットワーク上の同一ＩＤソフトの複数インストールを防止できる。このようにセキュリティ向上の様々な効果がある。

【図面の簡単な説明】

【図１】本発明の実施例の光ディスクの工程図

【図２】本発明の実施例のパルスレーザーによるトリミングの断面図

【図３】本発明の実施例のトリミング部の信号再生波形図

【図４】本発明の実施例の再生装置のブロック図

【図５】（ａ）本発明のＢＣＡ部の再生信号波形図
（ｂ）本発明のＢＣＡ部の寸法関係図

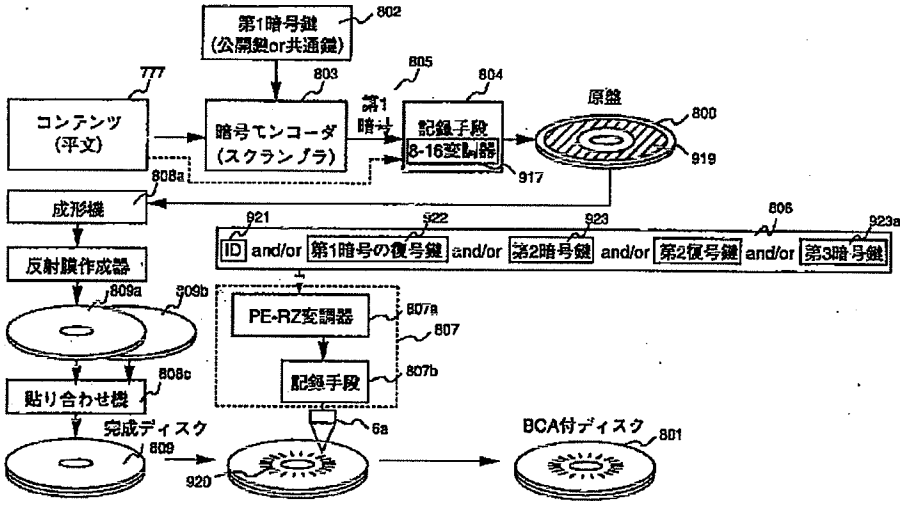
【図６】本発明の実施例の暗号通信の方法とパスワードによる暗号鍵の方法を示した図

【図７】本発明のＢＣＡのフォーマット図

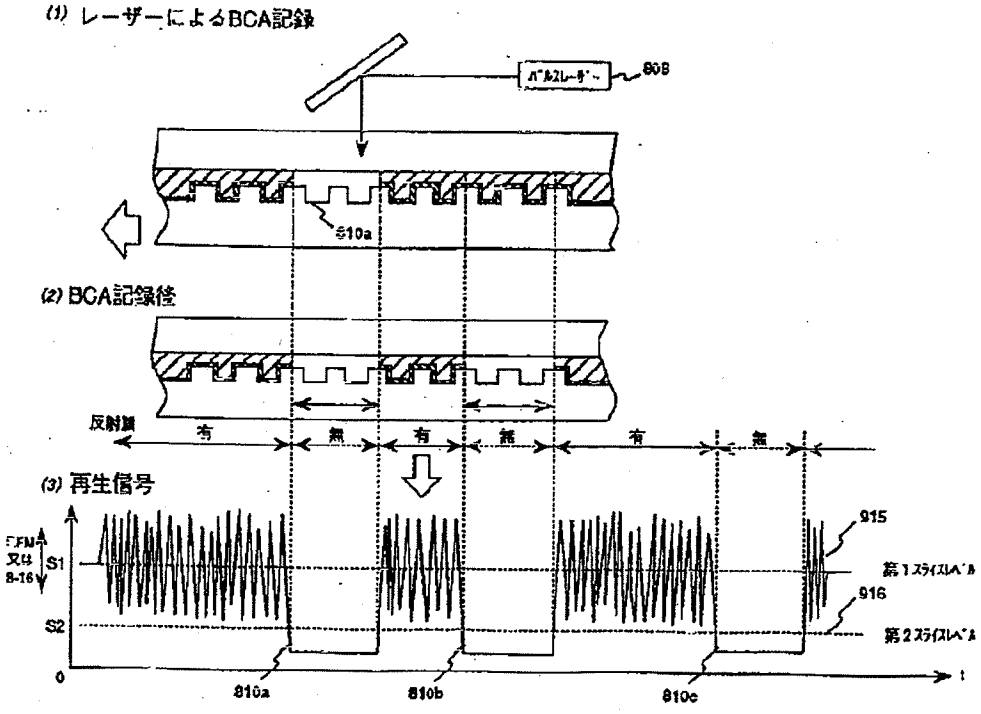
【図８】本発明の実施例の暗号通信の方法とパスワードによる暗号解鍵の方法を示した図
【図９】本発明の実施例のコンテンツ部分を使用許可したディスクの動作手順図
【図１０】本発明の実施例のＲＡＭディスクにＢＣＡを記録した場合のブロック図
【図１１】本発明の実施例の不正コピー防止方式のブロック図
【図１２】本発明の実施例の不正コピー防止のフローチャート
【図１３】本発明の実施例のＢＣＡに商品バーコードを印刷した光ディスクの上面図と断面図
【図１４】本発明の実施例のＢＣＡ付ＲＯＭディスクとＰＯＳ端末を用いたＰＯＳ決済システムのブロック図
【図１５】本発明の実施例のプレス工場とソフト会社と販売店の暗号解除の流れ図
【図１６】本発明の実施例のディスクＩＤ等を用いた暗号データの暗号化復号化ステップのフローチャート
【図１７】本発明の実施例のディスクＩＤ等を用いた暗号データの暗号化復号化ステップのフローチャート
【図１８】本発明の実施例のＢＣＡを用いた通信暗号鍵の配布と暗号通信のフローチャート
【図１９】本発明の実施例のＢＣＡを用いた通信暗号鍵の配布と暗号通信のフローチャート
【図２０】本発明の実施例のＢＣＡを用いた通信暗号鍵の配布と暗号通信のフローチャート
【図２１】本発明の実施例のＢＣＡを用いた電子決済システムのフローチャート
【図２２】本発明の実施例のＢＣＡを用いた電子決済システムのフローチャート
【図２３】本発明の実施例のＢＣＡを用いた電子決済システムのフローチャート
【図２４】本発明の実施例のＢＣＡを用いた１枚のＲＡＭディスクに記録制限する記録再生方法のブロック図
【符号の説明】
８０１　ＢＣＡ付ディスク
８０２　固定鍵
８０３　暗号エンコーダ
８０４　記録手段
８０５　コンテンツ
８０６　ＩＤ
８０７　トリミング装置
８０８ａ　成形機
８０８ｂ　反射膜作成機
８０８ｃ　貼り合わせ機
８０９　完成ディスク
８０９ａ　片面ディスク
８０９ｂ　片面ディスク
８１１　プレス場
８１３　固定鍵
８１４　ＢＣＡ領域
８１５　ディスクＩＤ
８１６　第１暗号鍵（秘密鍵）
８１７　第２暗号鍵（秘密鍵）
８１８　接続アドレス
８１９　再生装置
８２０　ＢＣＡ再生部
８２１　パスワード発行センター
８２２　通信部
８２３　ネットワーク
８２４　暗号鍵ＤＢ
８２５　第１復号鍵
８２６　コンテンツ番号
８２７　第１暗号デコーダ
８２８　課金センター
８２９　第２復号鍵
８３０　課金情報
８３１　第２暗号エンコーダ
８３２　第２暗号デコーダ
８３３　時間情報
８３４　パスワード生成部
８３５　パスワード
８３６　パソコン
８３７　第３復号鍵
８３８　共通鍵
８３９　第３暗号鍵
８４０　第３暗号エンコーダ
８４１　第３暗号デコーダ
８４２　主暗号エンコーダ
８４３　主暗号デコーダ
８４４　主復号鍵
８４５　第１暗号デコーダ
８４６　暗号エンコーダ
８４７　暗号デコーダ
８４９　ＢＣＡデータ
８５０　書き込み層
８５１　文字
８５２　一般バーコード
８５３　復号器
８６０　第２暗号エンコーダ
８６１　第２暗号デコーダ
８６２　データ再生部
８６３　ＲＯＭ領域
８６４　追記領域
８６５　復号フローチャート
８９０　第２暗号演算器
８９４ａ　第１記録領域
９０８　インターネット
９０９　第１コンピュータ
９１０　第２コンピュータ

911　第3コンピュータ
912　第2暗号
913　復号鍵識別情報
914　復号鍵選別手段
915　第1スライスレベル
916　第2スライスレベル
917　PE-RZ変調器
918　透明基板
919　第1記録領域
920　第2記録領域
921　ディスクID
922　BCAフラグ
923　CPU
924　コントロールデータ
925　EFM復調
926　8-15変調復調
927　8-16変調復調
928　第1復調部
930　第2復調部
931　接続アドレス

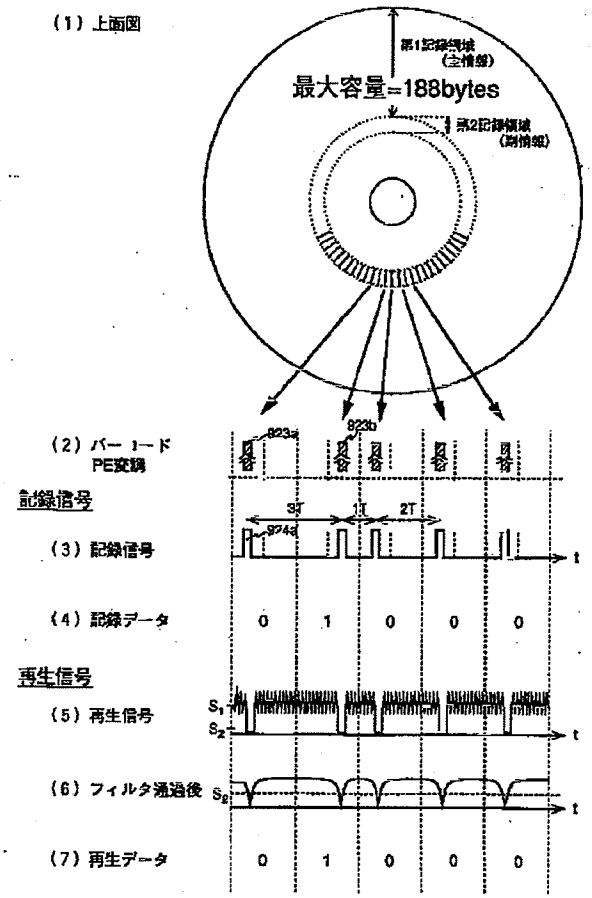
【図1】



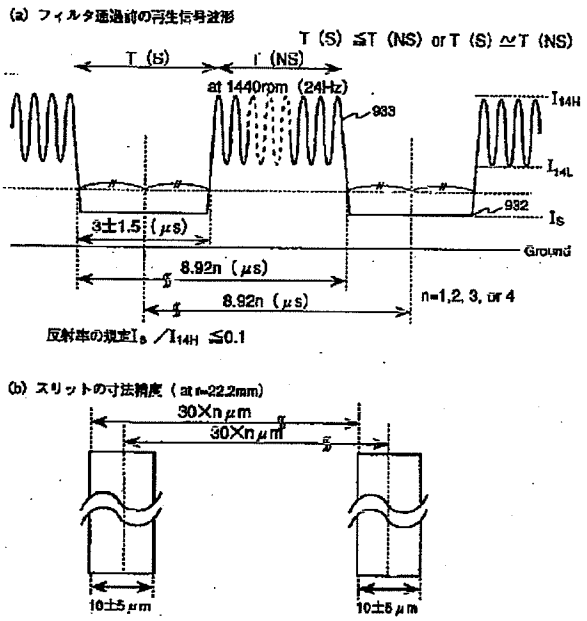
【図2】



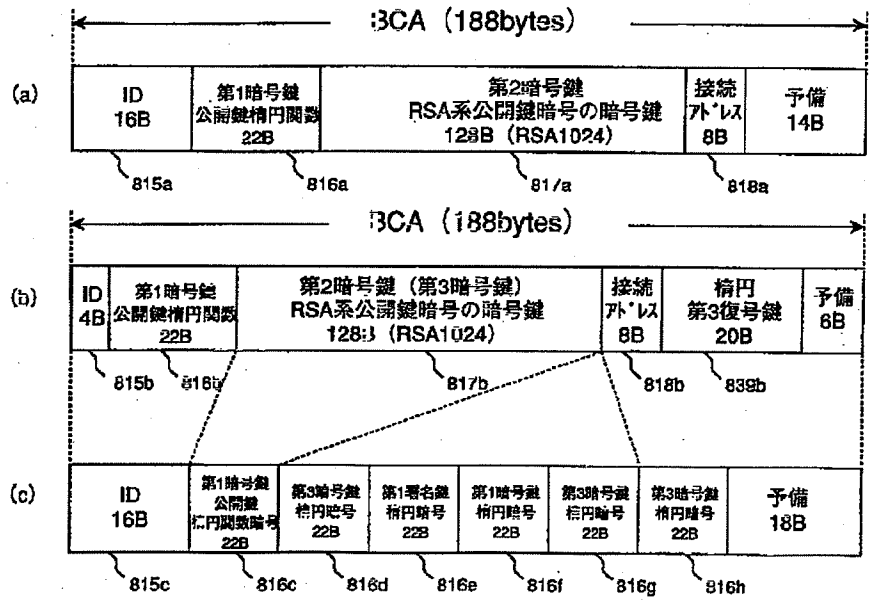
【図3】


(1) 上面図
第1記録領域
(主情報)
最大容量=188bytes
第2記録領域
(副情報)
(2) バーコード
PE変調
823a
823b
記録信号
3T
1T
2T
974a
(3) 記録信号
t
(4) 記録データ
0 1 0 0 0
再生信号
(5) 再生信号
S1
S2
t
(6) フィルタ通過後
S2
t
(7) 再生データ
0 1 0 0 0

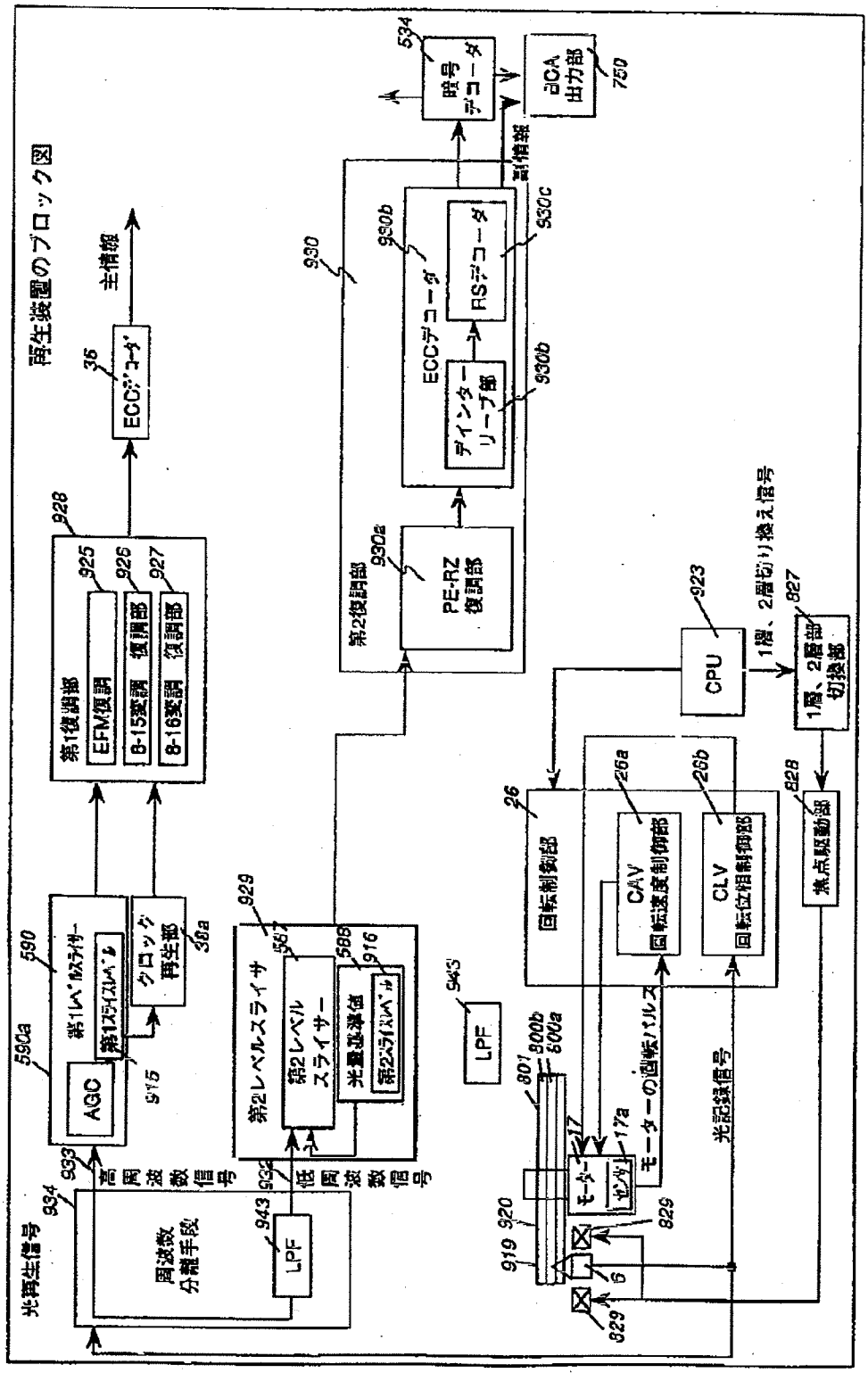
【図5】


(a) フィルタ通過前の再生信号波形
T (S) ≦T (NS) or T (S) ≒T (NS)
T (S)
T (NS)
at 1440rpm (24Hz)
933
I14H
I14L
932
IS
3±1.5 (μs)
Ground
8.92n (μs)
8.92n (μs)
n=1,2, 3, or 4
反射率の規定IS /I14H ≦0.1
(b) スリットの寸法精度 (at r=22.2mm)
30Xnμm
30Xnμm
10±5μm
10±5μm

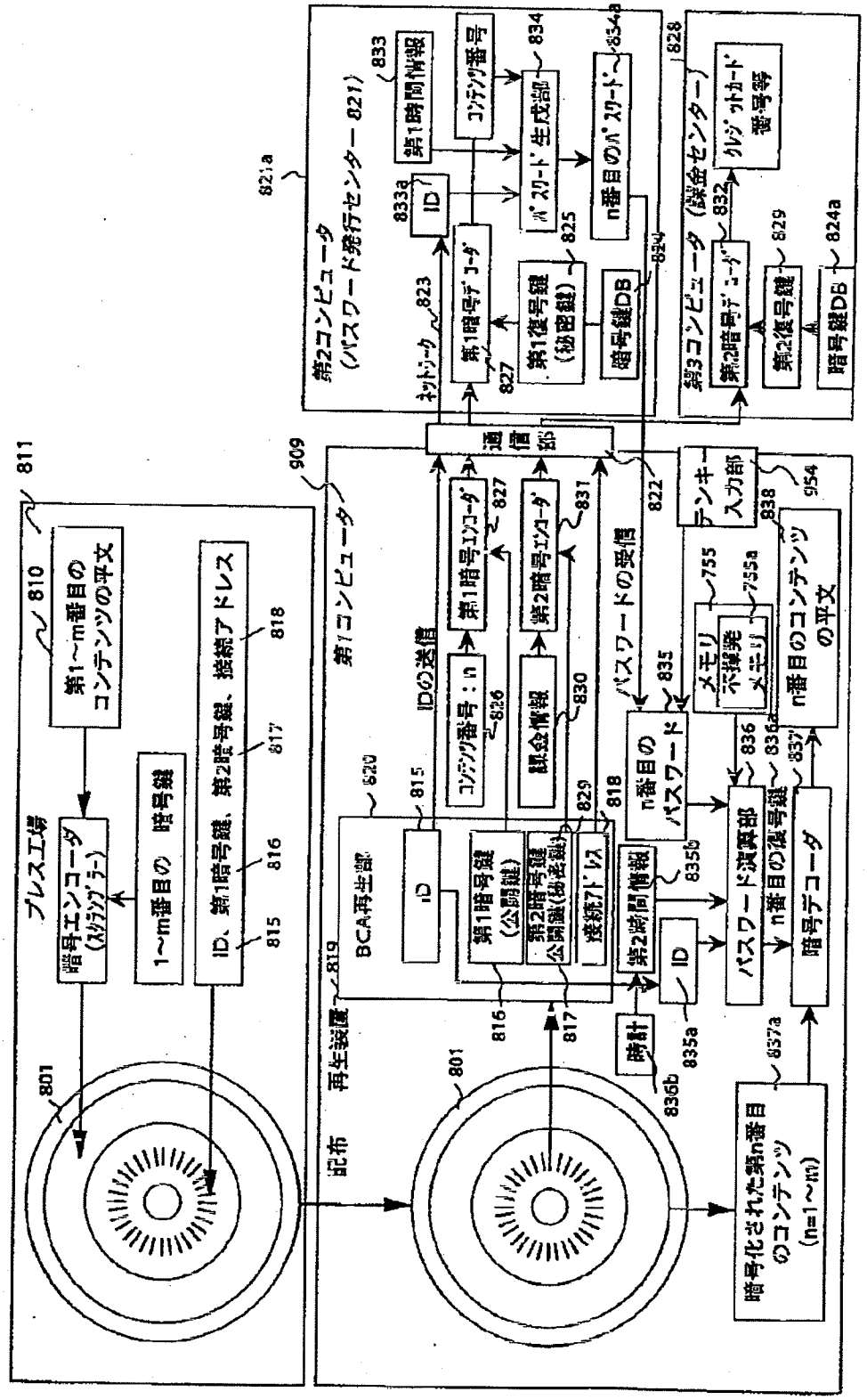
【図7】


BCA (188bytes)
(a)
ID
16B
第1暗号鍵
公開鍵楕円関数
22B
第2暗号鍵
RSA系公開鍵暗号の暗号鍵
128B (RSA1024)
接続
ｱﾄﾞﾚｽ
8B
予備
14B
815a
816a
817a
818a
BCA (188bytes)
(b)
ID
4B
第1暗号鍵
公開鍵楕円関数
22B
第2暗号鍵 (第3暗号鍵)
RSA系公開鍵暗号の暗号鍵
128B (RSA1024)
接続
ｱﾄﾞﾚｽ
8B
楕円
第3復号鍵
20B
予備
8B
815b
816b
817b
818b
839b
(c)
ID
16B
第1暗号鍵
公開鍵
楕円関数暗号
22B
第3暗号鍵
楕円暗号
22B
第1署名鍵
楕円暗号
22B
第1暗号鍵
楕円暗号
22B
第3暗号鍵
楕円暗号
22B
第3暗号鍵
楕円暗号
22B
予備
18B
815c
816c
816d
816e
816f
816g
816h

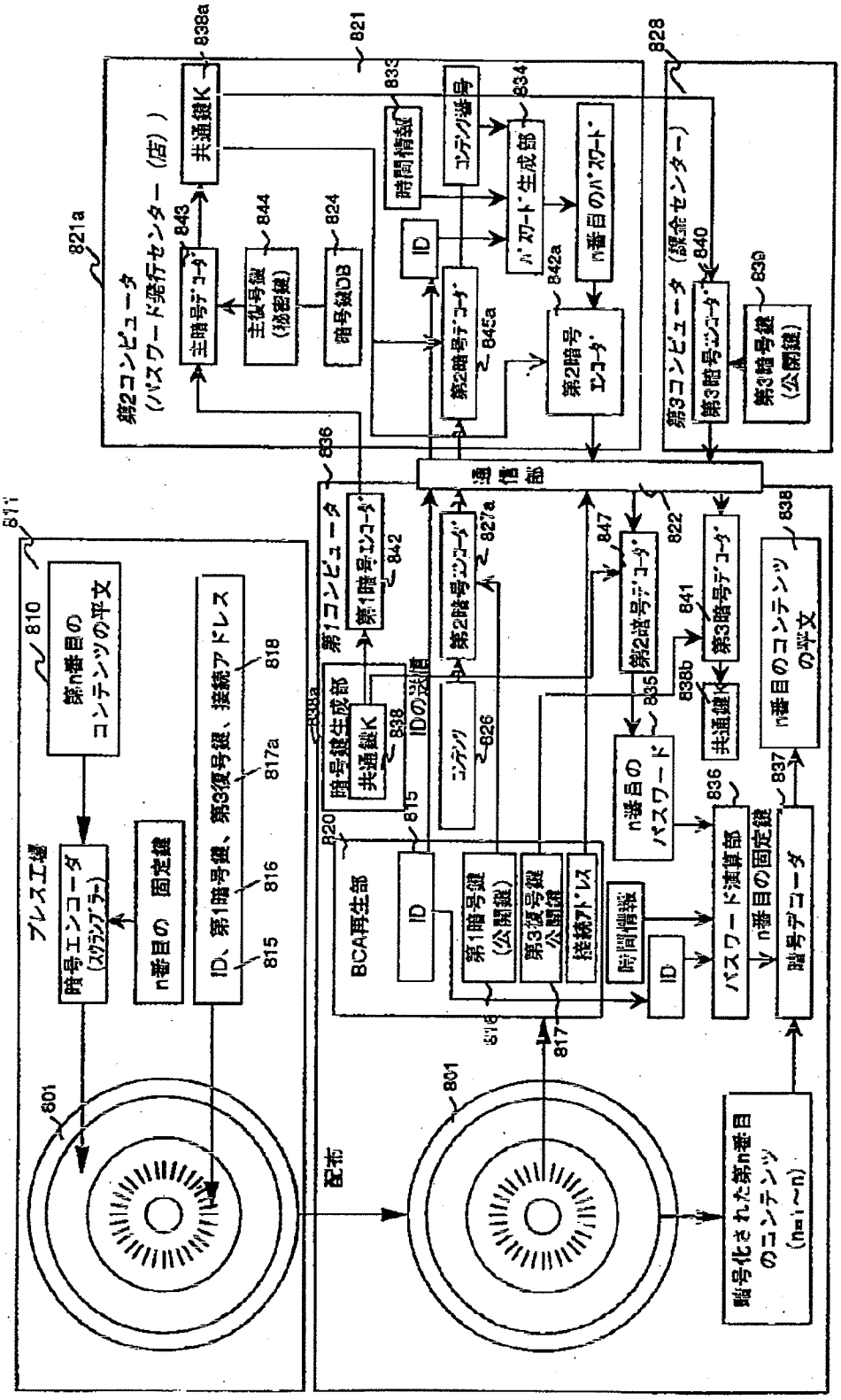
【図4】


再生装置のブロック図
光再生信号
周波数分離手段
LPF
高周波数信号
低周波数信号
AGC
第1レベルスライサー
第1スライスレベル
クロック再生部
第1復調部
EFM復調
8-15変調 復調部
8-16変調 復調部
ECCデコーダ
主情報
第2レベルスライサ
第2レベルスライサー
光量基準値
第2スライスレベル
第2復調部
PE-RZ復調部
ECCデコーダ
デインターリーブ部
RSデコーダ
副情報
暗号デコーダ
aCA出力部
CPU
1層、2層切り換え信号
1層、2層切換部
焦点駆動部
回転制御部
CAV回転速度制御部
CLV回転位相制御部
モーター
センサ
モーターの回転パルス
光記録信号

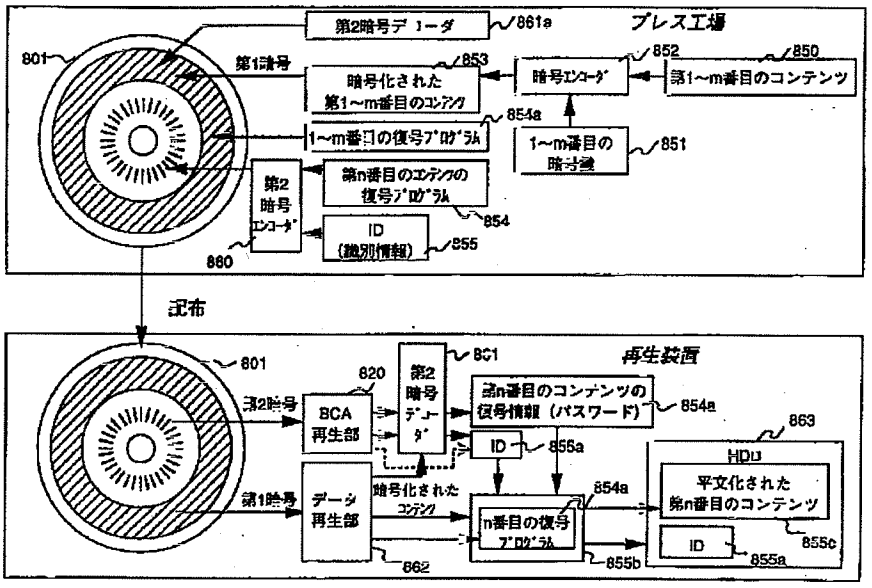
【図6】


プレス工場
暗号エンコーダ（スクランブラー）
第1～m番目のコンテンツの平文
1～m番目の 暗号鍵
ID、第1暗号鍵、第2暗号鍵、接続アドレス
811
810
801
815
816
817
818
記布
再生装置
第1コンピュータ
909
BCA再生部
820
819
ID
第1暗号鍵（公開鍵）
第2暗号鍵（秘密鍵）
接続アドレス
時計
835a
836b
IDの送信
コンテンツ番号：n
826
第1暗号エンコーダ
827
第2暗号エンコーダ
831
課金情報
830
829
通信部
822
パスワードの受信
n番目のパスワード
835
メモリ
755
755a
テンキー入力部
838
954
n番目のコンテンツの平文
836
836a
837
パスワード演算部
n番目の復号鍵
837a
暗号デコーダ
暗号化された第n番目のコンテンツ
(n=1～m)
第2コンピュータ（パスワード発行センター 821）
821a
ネットワーク
823
第1暗号デコーダ
827
第1復号鍵（秘密鍵）
825
暗号鍵DB
824
第1時間情報
833
ID
833a
コンテンツ番号
834
パスワード生成部
n番目のパスワード
834a
第3コンピュータ（課金センター）
828
第3暗号デコーダ
832
第2復号鍵
829
暗号鍵DB
824a
クレジットカード番号等

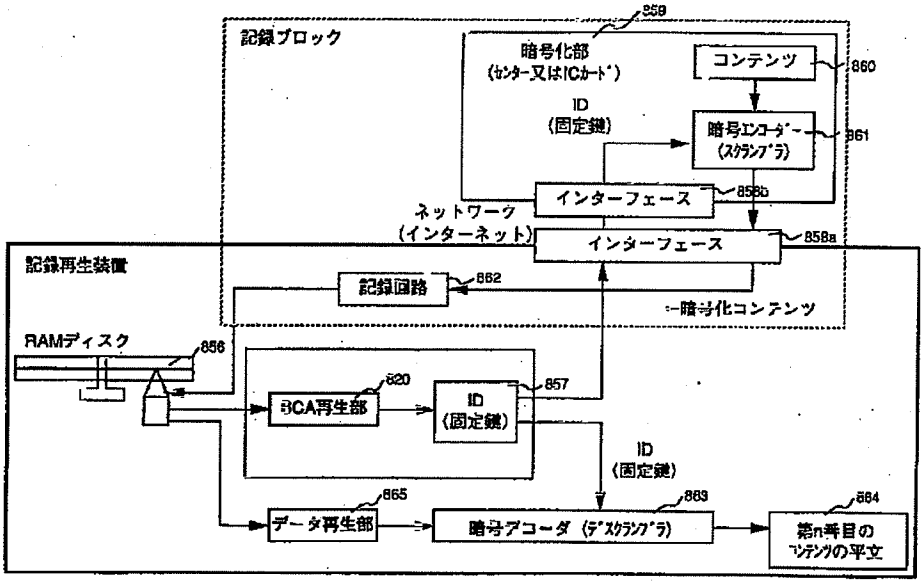
【図8】


第2コンピュータ
(パスワード発行センター(店))
821a
共通鍵K
838a
主暗号ﾃﾞｺｰﾀﾞ
843
主復号鍵
(秘密鍵)
844
暗号鍵DB
824
821
時間情報
833
コンテンツ番号
834
ID
パスワード生成部
n番目のパスワード
842a
第2暗号ﾃﾞｺｰﾀﾞ
845a
第2暗号
エンコーダ
828
第3コンピュータ(課金センター)
第3暗号ｴﾝｺｰﾀﾞ
840
第3暗号鍵
(公開鍵)
839
通信部
836
第1コンピュータ
第1暗号ｴﾝｺｰﾀﾞ
842
第2暗号ｴﾝｺｰﾀﾞ
827a
847
第2復号ﾃﾞｺｰﾀﾞ
822
第3暗号ﾃﾞｺｰﾀﾞ
841
838b
共通鍵K
838
IDの送信
ｺﾝﾃﾝﾂ
826
暗号鍵生成部
共通鍵K
838a
835
n番目の
パスワード
BCA再生部
ID
第1暗号鍵
(公開鍵)
第3復号鍵
公開鍵
接続ｱﾄﾞﾚｽ
時間情報
ID
820
815
816
817
パスワード演算部
n番目の固定鍵
836
837
暗号ﾃﾞｺｰﾀﾞ
n番目のコンテンツ
の平文
838
プレス工場
811
第n番目の
コンテンツの平文
810
暗号エンコーダ
(スクランブラー)
n番目の 固定鍵
ID、第1暗号鍵、第3復号鍵、接続アドレス
818
817a
815
816
801
配布
801
暗号化された第n番目
のコンテンツ
(n=1～n)

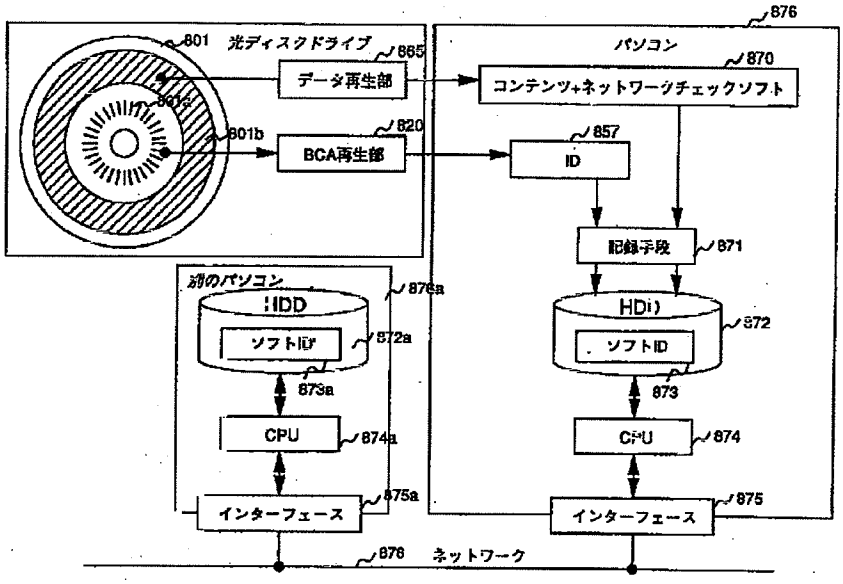
【図9】


第2暗号データ
861a
プレス工場
801
第1暗号
暗号化された
第1～m番目のコンテンツ
853
暗号エンコーダ
852
第1～m番目のコンテンツ
850
1～m番目の復号プログラム
854a
1～m番目の
暗号鍵
851
第2
暗号
エンコーダ
第n番目のコンテンツの
復号プログラム
854
ID
(識別情報)
855
860
記布
801
再生装置
第2暗号
820
BCA
再生部
第2
暗号
データ
861
第n番目のコンテンツの
復号情報（パスワード）
854a
ID
855a
863
HDD
平文化された
第n番目のコンテンツ
855c
第1暗号
データ
再生部
暗号化された
コンテンツ
862
n番目の復号
プログラム
854a
855b
ID
855a

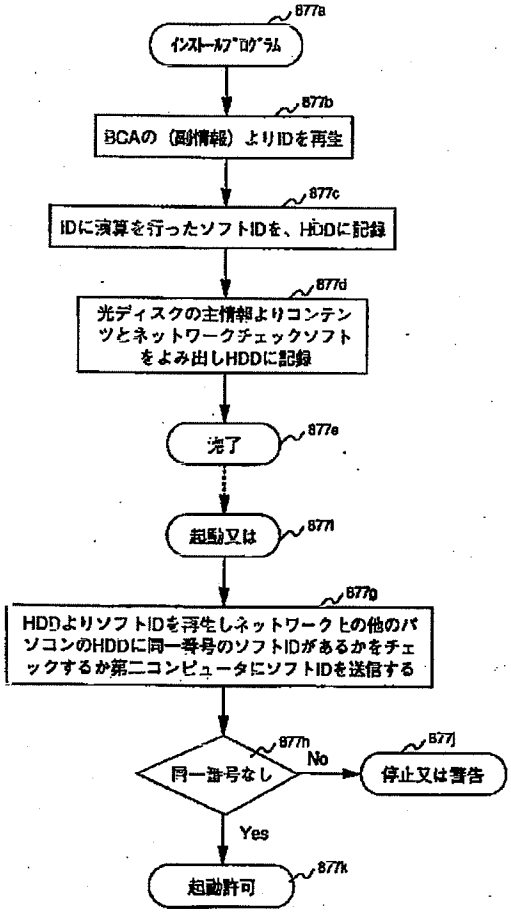
【図10】


記録ブロック
859
暗号化部
(センター又はICカード)
コンテンツ
860
ID
(固定鍵)
暗号エンコーダ
(スクランブラ)
861
インターフェース
858b
ネットワーク
(インターネット)
インターフェース
858a
記録再生装置
記録回路
862
暗号化コンテンツ
RAMディスク
856
BCA再生部
820
ID
(固定鍵)
857
ID
(固定鍵)
データ再生部
865
暗号デコーダ（デスクランブラ）
863
第n番目の
コンテンツの平文
864

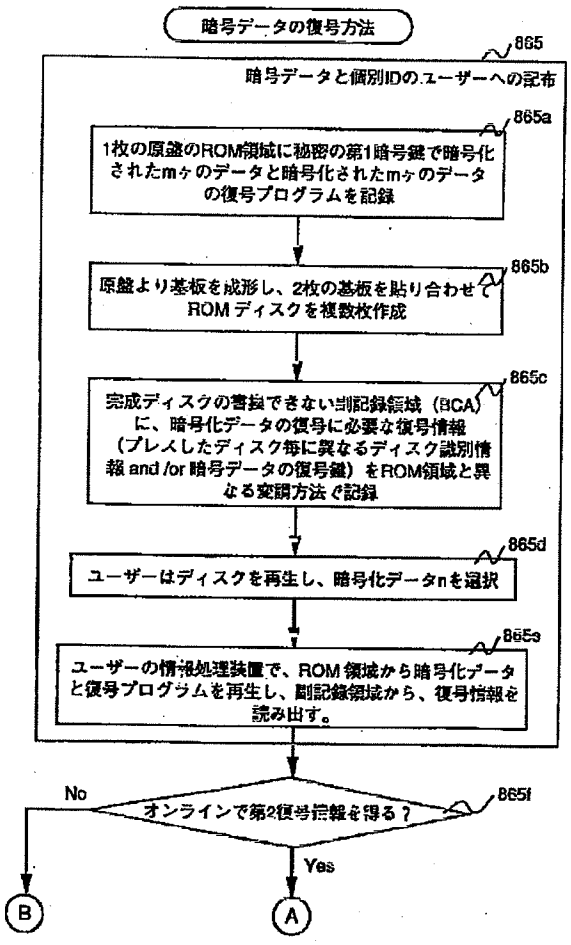
【図１１】


876
801 光ディスクドライブ
865
データ再生部
パソコン
870
コンテンツ+ネットワークチェックソフト
801a
801b
820
BCA再生部
857
ID
記録手段
871
別のパソコン
876a
HDD
ソフトID
872a
873a
HDD
ソフトID
872
873
CPU
874a
CPU
874
インターフェース
875a
インターフェース
875
876 ネットワーク

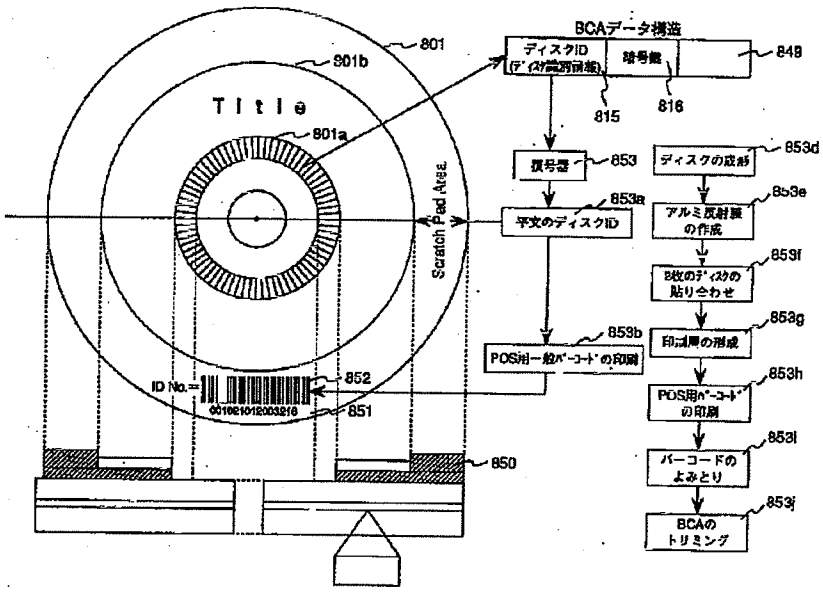
【図１２】


877a
インストールプログラム
877b
BCAの（副情報）よりIDを再生
877c
IDに演算を行ったソフトIDを、HDDに記録
877d
光ディスクの主情報よりコンテンツとネットワークチェックソフトをよみ出しHDDに記録
877e
完了
877f
起動又は
877g
HDDよりソフトIDを再生しネットワーク上の他のパソコンのHDDに同一番号のソフトIDがあるかをチェックするか第二コンピュータにソフトIDを送信する
877h
同一番号なし
No
877j
停止又は警告
Yes
877k
起動許可

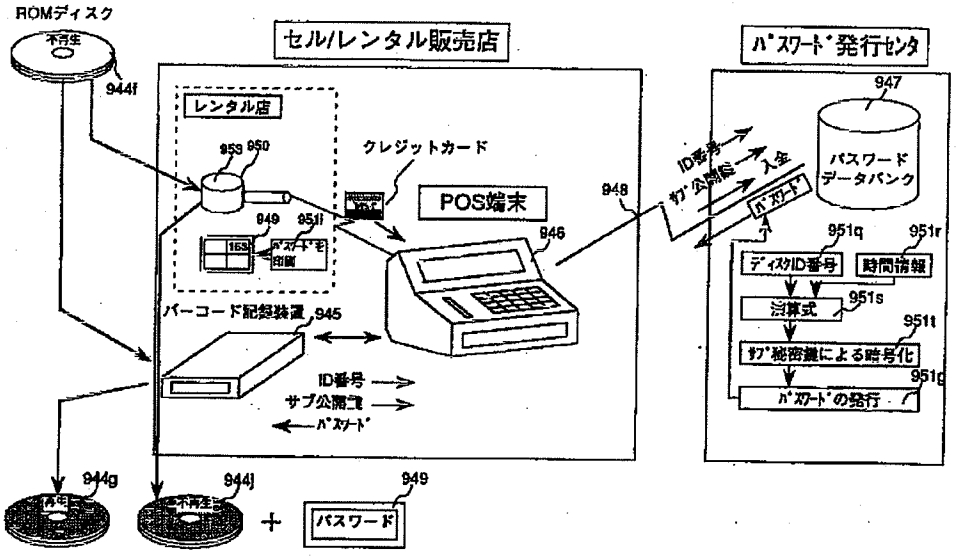
【図１６】


暗号データの復号方法
865
暗号データと個別IDのユーザーへの記布
865a
1枚の原盤のROM領域に秘密の第1暗号鍵で暗号化されたmヶのデータと暗号化されたmヶのデータの復号プログラムを記録
865b
原盤より基板を成形し、2枚の基板を貼り合わせてROMディスクを複数枚作成
865c
完成ディスクの書換できない副記録領域（BCA）に、暗号化データの復号に必要な復号情報（プレスしたディスク毎に異なるディスク識別情報 and /or 暗号データの復号鍵）をROM領域と異なる変調方法で記録
865d
ユーザーはディスクを再生し、暗号化データnを選択
865e
ユーザーの情報処理装置で、ROM領域から暗号化データと復号プログラムを再生し、副記録領域から、復号情報を読み出す。
No
865f
オンラインで第2復号情報を得る？
Yes
B
A

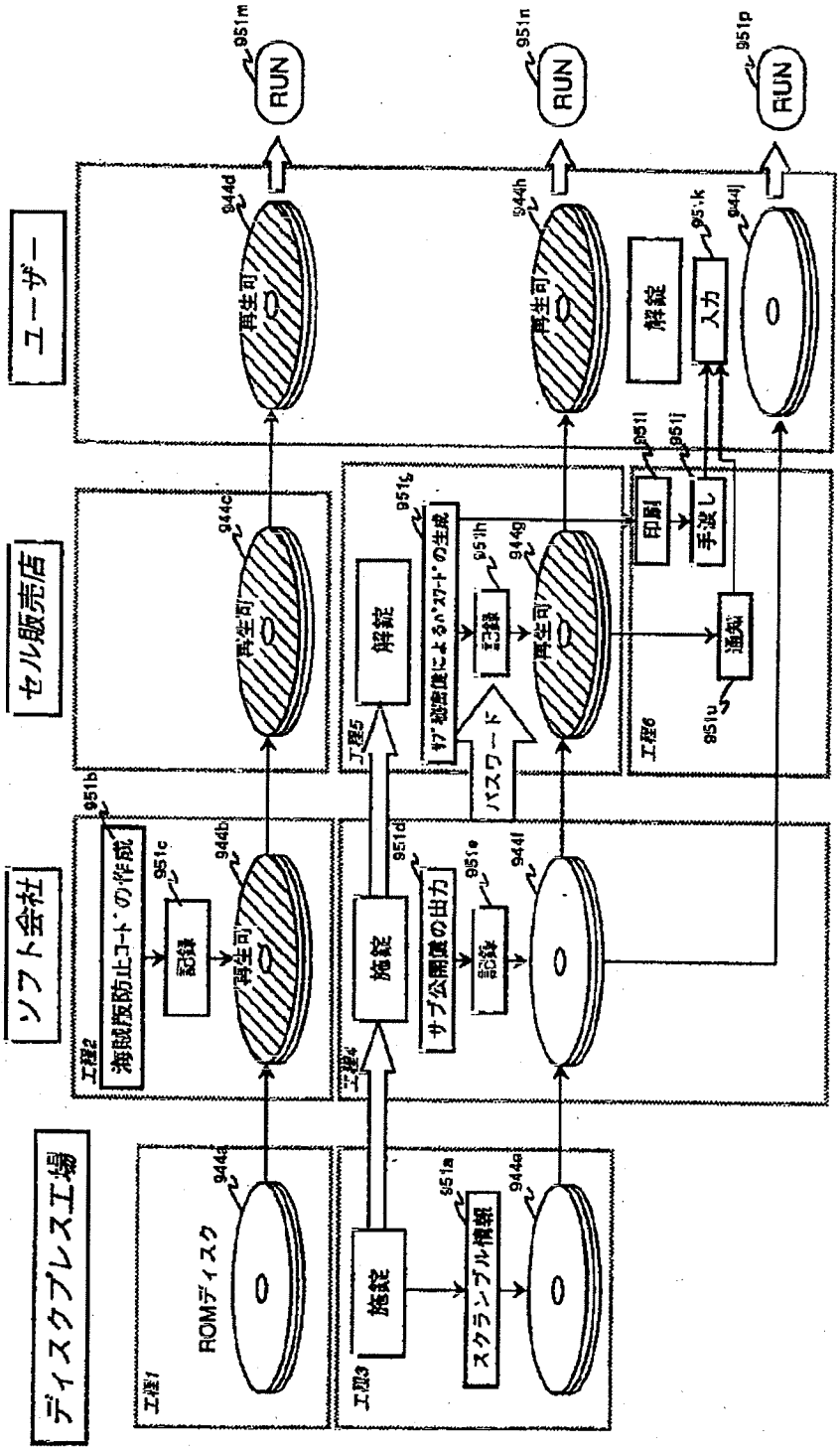
【図13】


BCAデータ構造
ディスクID
暗号鍵
848
815
816
801
801b
Title
801a
Scratch Pad Area
853
853a
平文のディスクID
853d
ディスクの成形
853e
アルミ反射膜の作成
853f
8枚のディスクの貼り合わせ
853g
印刷層の形成
853h
POS用バーコードの印刷
853i
バーコードの読みとり
853j
BCAのトリミング
853b
POS用一般バーコードの印刷
ID No.=
852
851
850

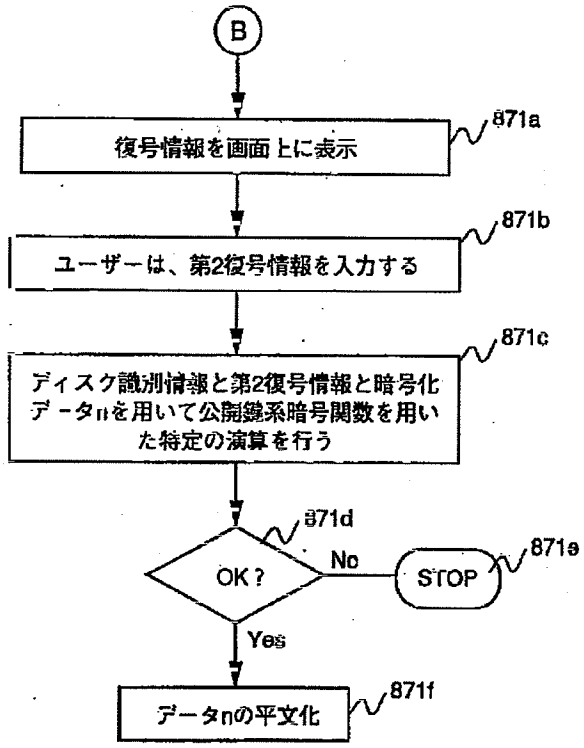
【図14】


ROMディスク
不再生
944f
セル/レンタル販売店
パスワード発行センタ
レンタル店
クレジットカード
POS端末
バーコード記録装置
945
946
948
947
パスワードデータバンク
ID番号
サブ公開鍵
パスワード
入金
951q
951r
ディスクID番号
時間情報
951s
計算式
951t
サブ秘密鍵による暗号化
951g
パスワードの発行
944g
944j
949
パスワード

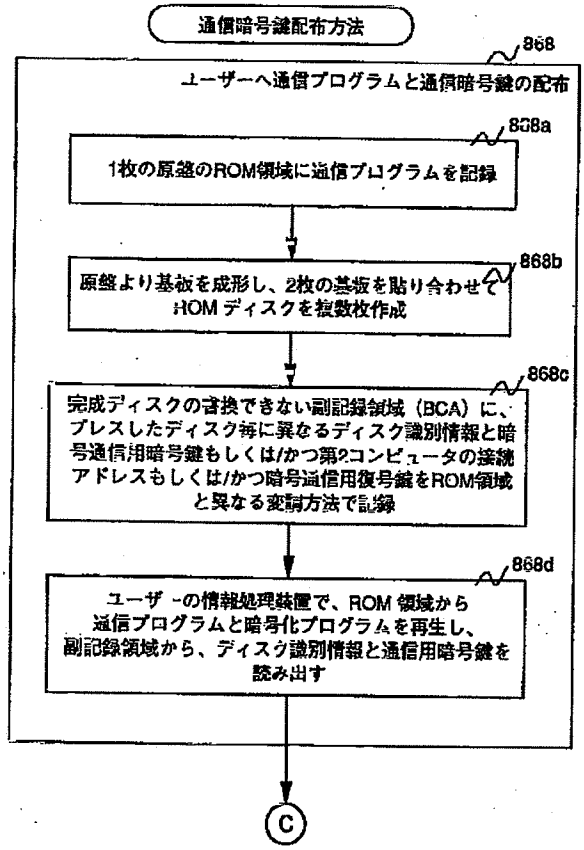
【図15】


ディスクプレス工場
ソフト会社
セル販売店
ユーザー
ROMディスク
施錠
スクランブル情報
海賊版防止コードの作成
記録
再生可
サブ公開鍵の出力
パスワード
サブ秘密鍵によるカラオケの生成
解錠
印刷
手渡し
入力
通知
RUN
工程1
工程2
工程3
工程4
工程5
工程6

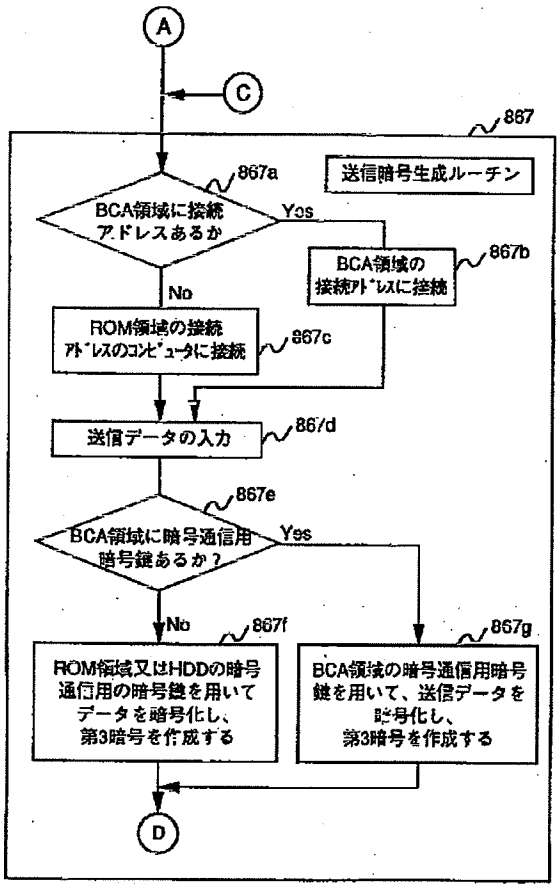
【図17】


B
復号情報を画面上に表示
871a
ユーザーは、第2復号情報を入力する
871b
ディスク識別情報と第2復号情報と暗号化データnを用いて公開鍵系暗号関数を用いた特定の演算を行う
871c
871d
OK?
No
STOP
871e
Yes
データnの平文化
871f

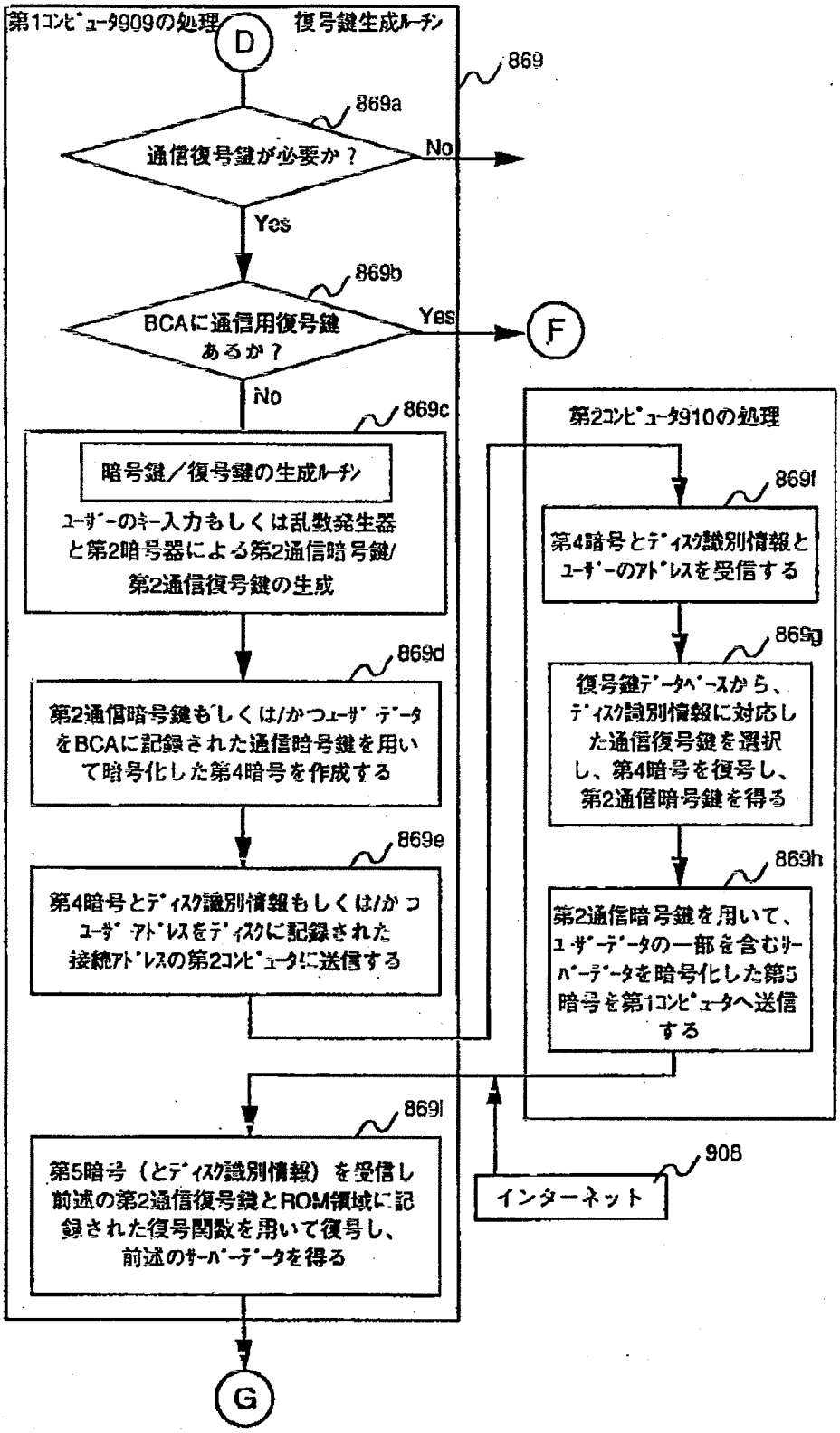
【図18】


通信暗号鍵配布方法
868
ユーザーへ通信プログラムと通信暗号鍵の配布
868a
1枚の原盤のROM領域に通信プログラムを記録
868b
原盤より基板を成形し、2枚の基板を貼り合わせてROMディスクを複数枚作成
868c
完成ディスクの書換できない副記録領域（BCA）に、プレスしたディスク毎に異なるディスク識別情報と暗号通信用暗号鍵もしくは/かつ第2コンピュータの接続アドレスもしくは/かつ暗号通信用復号鍵をROM領域と異なる変調方法で記録
868d
ユーザーの情報処理装置で、ROM領域から通信プログラムと暗号化プログラムを再生し、副記録領域から、ディスク識別情報と通信用暗号鍵を読み出す
C

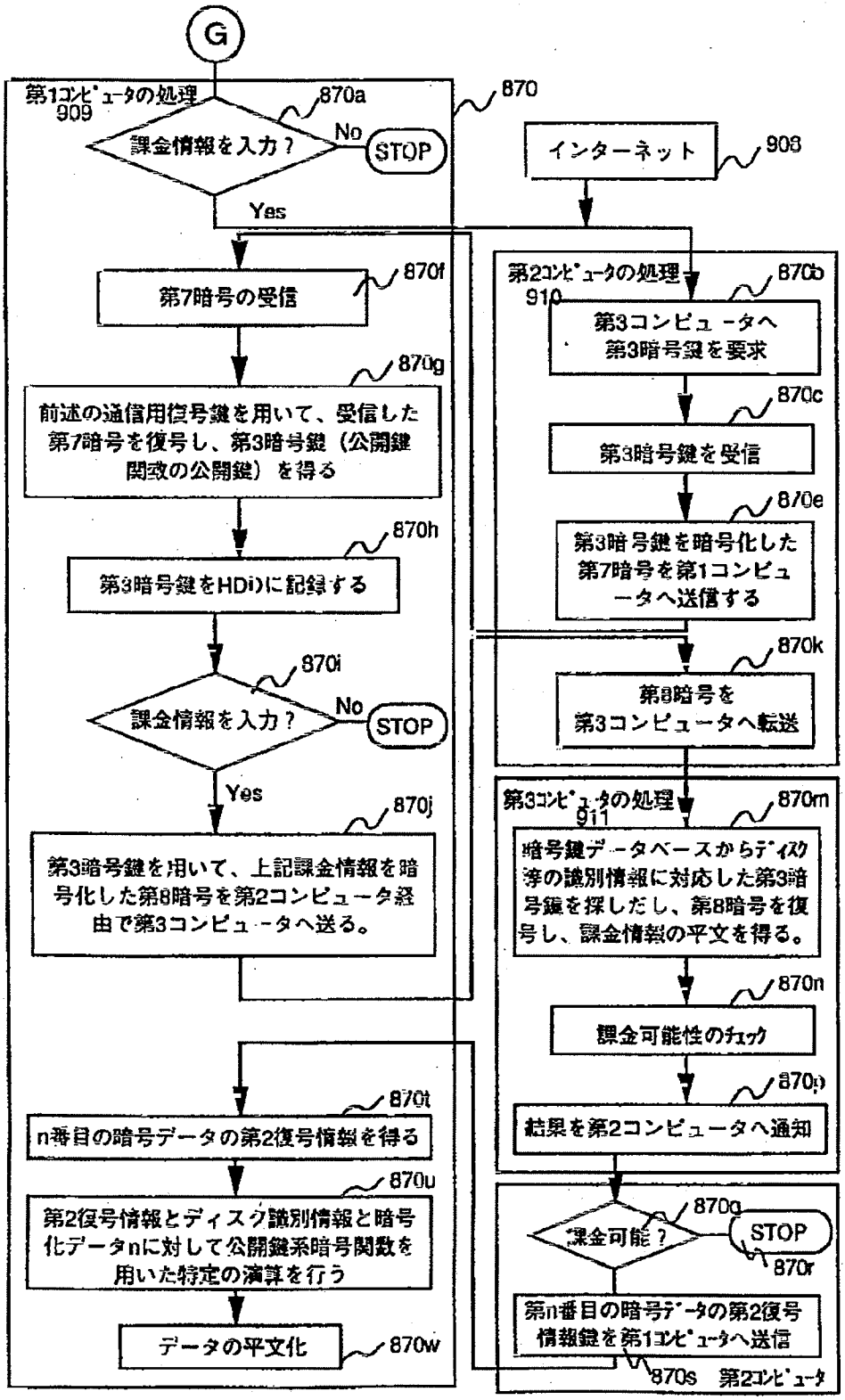
【図19】


A
C
867
867a
送信暗号生成ルーチン
BCA領域に接続アドレスあるか
Yes
867b
BCA領域の接続ｱﾄﾞﾚｽに接続
No
ROM領域の接続ｱﾄﾞﾚｽのｺﾝﾋﾟｭｰﾀに接続
867c
送信データの入力
867d
867e
BCA領域に暗号通信用暗号鍵あるか？
Yes
No
867f
867g
ROM領域又はHDDの暗号通信用の暗号鍵を用いてデータを暗号化し、第3暗号を作成する
BCA領域の暗号通信用暗号鍵を用いて、送信データを暗号化し、第3暗号を作成する
D

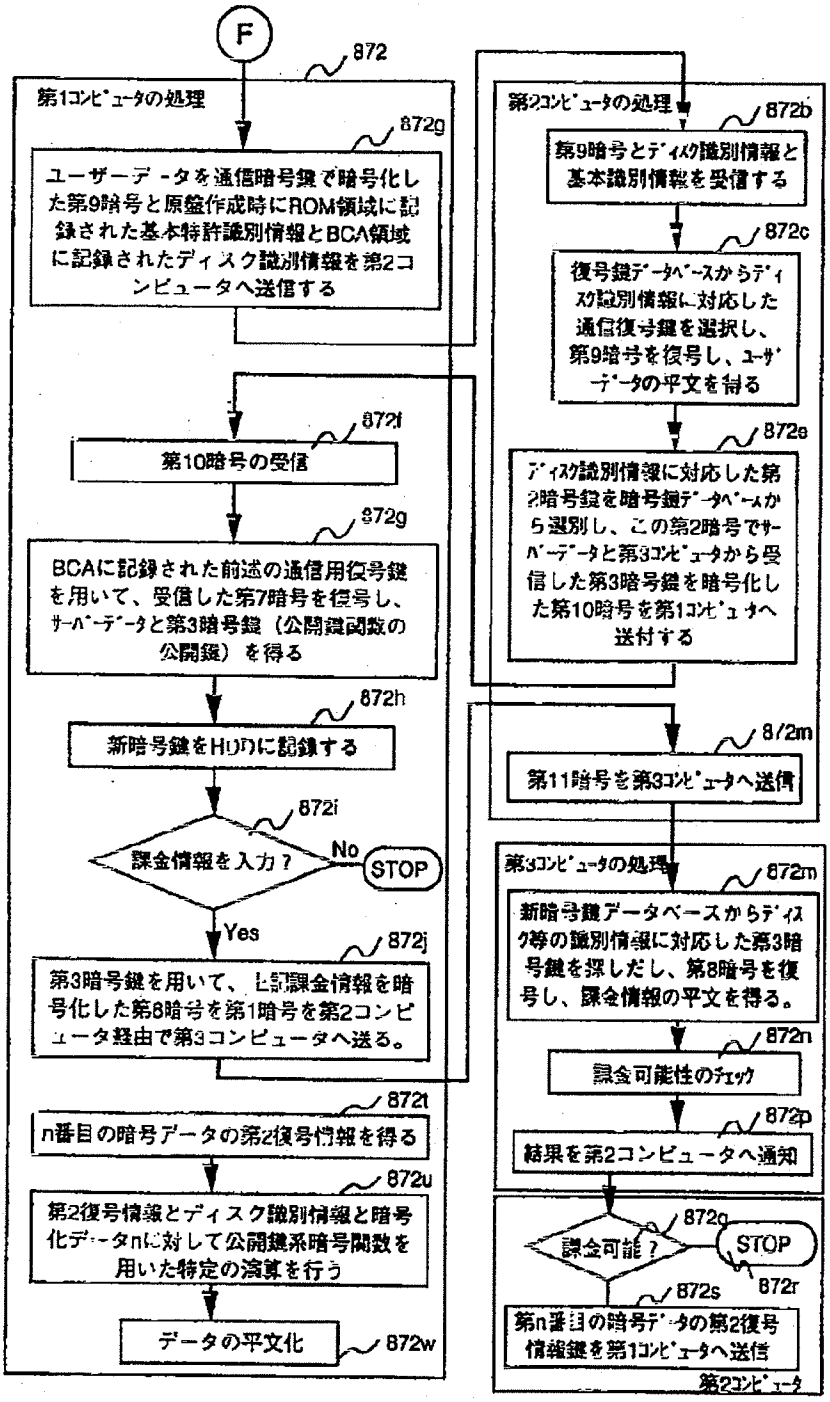
【図20】


第1ｺﾝﾋﾟｭｰﾀ909の処理
復号鍵生成ﾙｰﾁﾝ
D
869
869a
通信復号鍵が必要か？
No
Yes
869b
BCAに通信用復号鍵あるか？
Yes
F
No
869c
暗号鍵／復号鍵の生成ﾙｰﾁﾝ
ﾕｰｻﾞｰのｷｰ入力もしくは乱数発生器と第2暗号器による第2通信暗号鍵/第2通信復号鍵の生成
869d
第2通信暗号鍵もしくは/かつﾕｰｻﾞｰﾃﾞｰﾀをBCAに記録された通信暗号鍵を用いて暗号化した第4暗号を作成する
869e
第4暗号とﾃﾞｨｽｸ識別情報もしくは/かつﾕｰｻﾞｰｱﾄﾞﾚｽをﾃﾞｨｽｸに記録された接続ｱﾄﾞﾚｽの第2ｺﾝﾋﾟｭｰﾀに送信する
869i
第5暗号（とﾃﾞｨｽｸ識別情報）を受信し前述の第2通信復号鍵とROM領域に記録された復号関数を用いて復号し、前述のｻｰﾊﾞｰﾃﾞｰﾀを得る
G
第2ｺﾝﾋﾟｭｰﾀ910の処理
869f
第4暗号とﾃﾞｨｽｸ識別情報とﾕｰｻﾞｰのｱﾄﾞﾚｽを受信する
869g
復号鍵ﾃﾞｰﾀﾍﾞｰｽから、ﾃﾞｨｽｸ識別情報に対応した通信復号鍵を選択し、第4暗号を復号し、第2通信暗号鍵を得る
869h
第2通信暗号鍵を用いて、ﾕｻﾞｰﾃﾞｰﾀの一部を含むｻｰﾊﾞｰﾃﾞｰﾀを暗号化した第5暗号を第1ｺﾝﾋﾟｭｰﾀへ送信する
908
インターネット

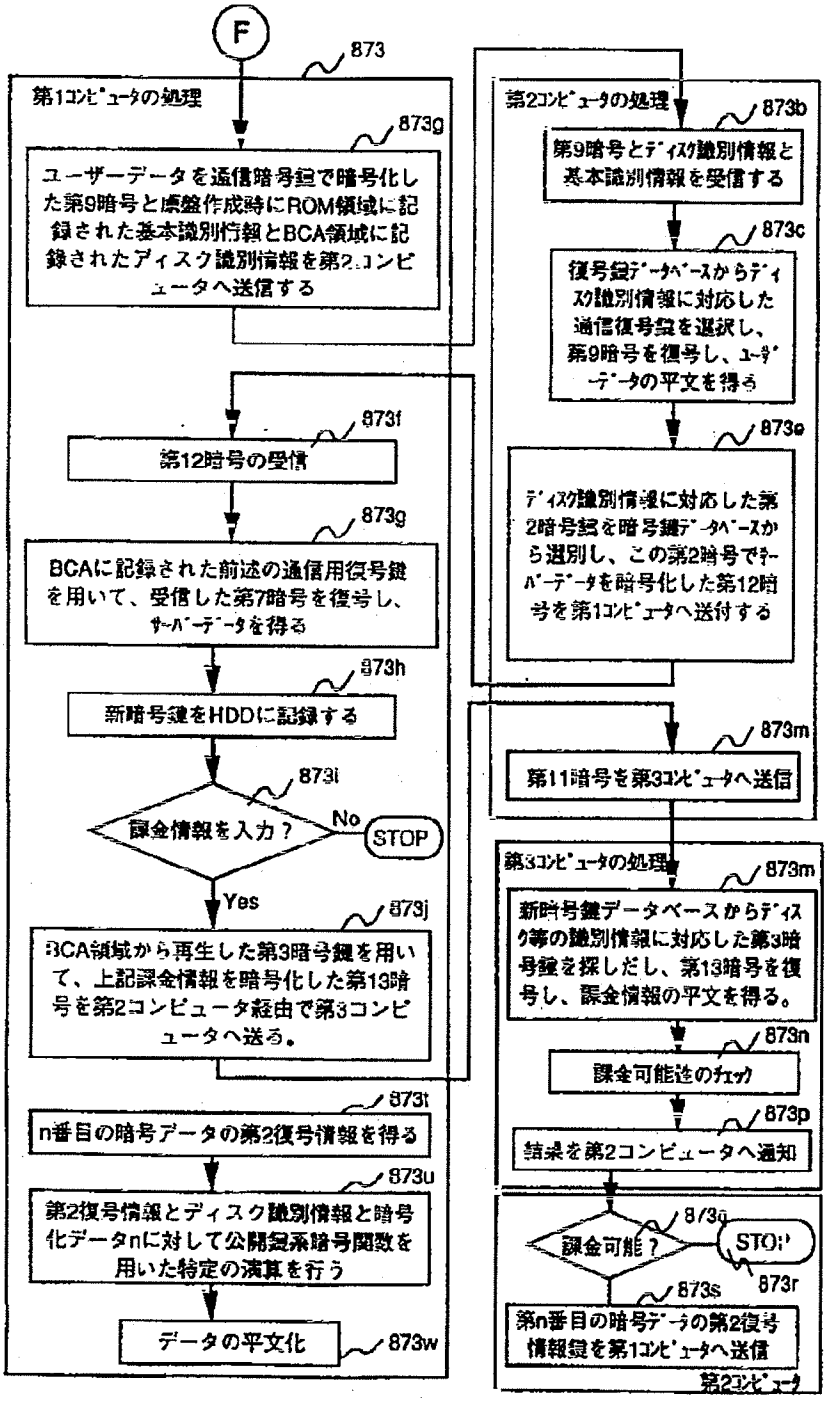
【図21】


G
第1コンピュータの処理
909
870a
課金情報を入力？
No
STOP
Yes
870
インターネット
903
第7暗号の受信
870f
第2コンピュータの処理
910
870b
第3コンピュータへ第3暗号鍵を要求
870c
第3暗号鍵を受信
870e
第3暗号鍵を暗号化した第7暗号を第1コンピュータへ送信する
870g
前述の通信用復号鍵を用いて、受信した第7暗号を復号し、第3暗号鍵（公開鍵関数の公開鍵）を得る
870h
第3暗号鍵をHDiに記録する
870k
第8暗号を第3コンピュータへ転送
870i
課金情報を入力？
No
STOP
Yes
870j
第3暗号鍵を用いて、上記課金情報を暗号化した第8暗号を第2コンピュータ経由で第3コンピュータへ送る。
第3コンピュータの処理
911
870m
暗号鍵データベースからディスク等の識別情報に対応した第3暗号鍵を探しだし、第8暗号を復号し、課金情報の平文を得る。
870n
課金可能性のチェック
870p
結果を第2コンピュータへ通知
870t
n番目の暗号データの第2復号情報を得る
870u
第2復号情報とディスク識別情報と暗号化データnに対して公開鍵系暗号関数を用いた特定の演算を行う
870q
課金可能？
STOP
870r
第n番目の暗号データの第2復号情報鍵を第1コンピュータへ送信
データの平文化
870w
870s
第2コンピュータ

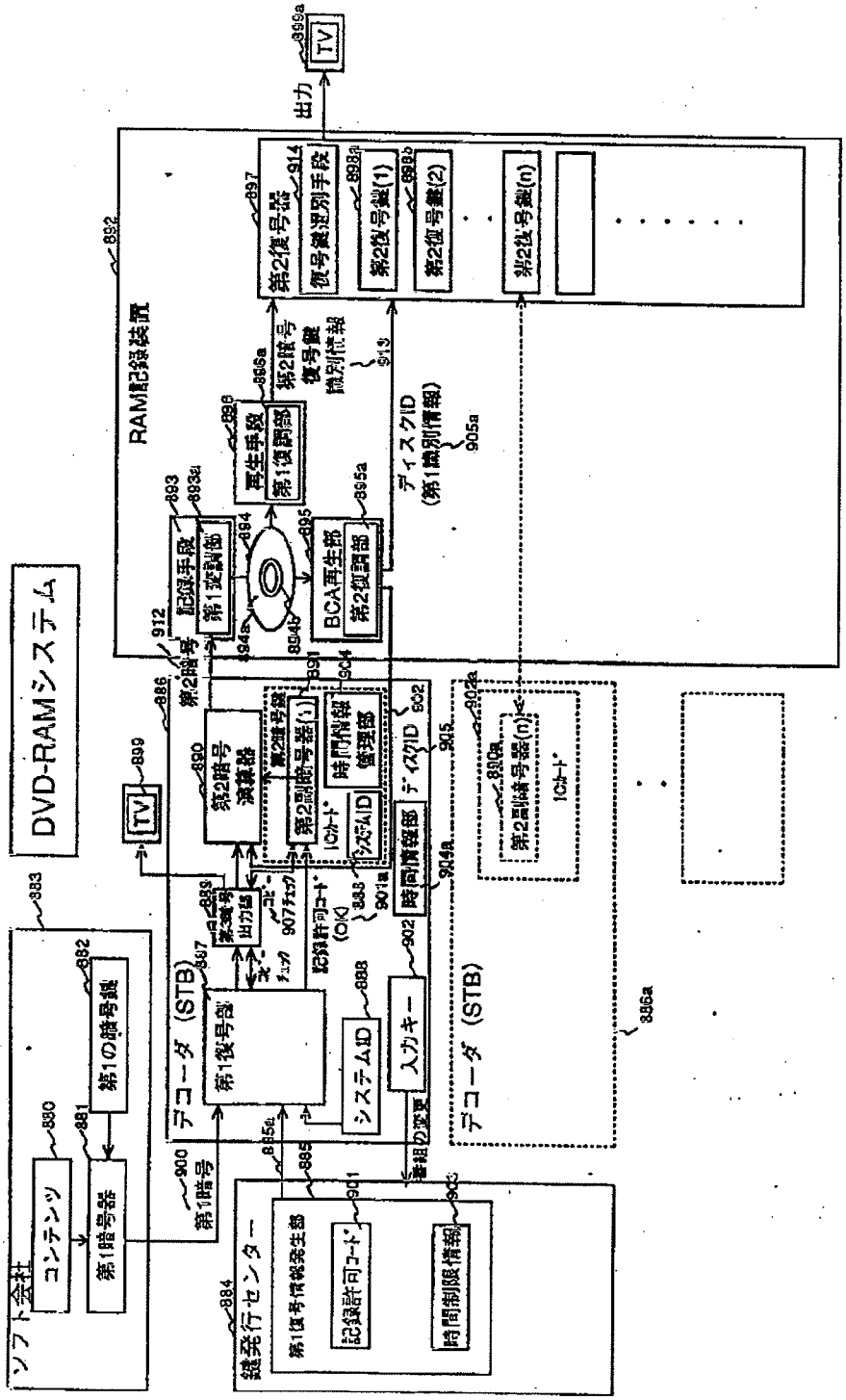
【図22】


F
872
第1コンピュータの処理
872g
ユーザーデータを通信暗号鍵で暗号化した第9暗号と原盤作成時にROM領域に記録された基本特許識別情報とBCA領域に記録されたディスク識別情報を第2コンピュータへ送信する
872i
第10暗号の受信
872g
BCAに記録された前述の通信用復号鍵を用いて、受信した第7暗号を復号し、サーバーデータと第3暗号鍵（公開鍵関数の公開鍵）を得る
872h
新暗号鍵をHDDに記録する
872i
課金情報を入力？
No
STOP
Yes
872j
第3暗号鍵を用いて、上記課金情報を暗号化した第8暗号を第1暗号を第2コンピュータ経由で第3コンピュータへ送る。
872t
n番目の暗号データの第2復号情報を得る
872u
第2復号情報とディスク識別情報と暗号化データnに対して公開鍵系暗号関数を用いた特定の演算を行う
データの平文化
872w
第2コンピュータの処理
872b
第9暗号とディスク識別情報と基本識別情報を受信する
872c
復号鍵データベースからディスク識別情報に対応した通信復号鍵を選択し、第9暗号を復号し、ユーザーデータの平文を得る
872e
ディスク識別情報に対応した第2暗号鍵を暗号鍵データベースから選別し、この第2暗号でサーバーデータと第3コンピュータから受信した第3暗号鍵を暗号化した第10暗号を第1コンピュータへ送付する
872m
第11暗号を第3コンピュータへ送信
第3コンピュータの処理
872m
新暗号鍵データベースからディスク等の識別情報に対応した第3暗号鍵を探しだし、第8暗号を復号し、課金情報の平文を得る。
872n
課金可能性のチェック
872p
結果を第2コンピュータへ通知
872q
課金可能？
STOP
872r
872s
第n番目の暗号データの第2復号情報鍵を第1コンピュータへ送信
第2コンピュータ

【図23】


F
873
第1コンピュータの処理
873g
ユーザーデータを通信暗号鍵で暗号化した第9暗号と原盤作成時にROM領域に記録された基本識別情報とBCA領域に記録されたディスク識別情報を第2コンピュータへ送信する
873f
第12暗号の受信
873g
BCAに記録された前述の通信用復号鍵を用いて、受信した第7暗号を復号し、サーバーデータを得る
873h
新暗号鍵をHDDに記録する
873i
課金情報を入力？
No
STOP
Yes
873j
BCA領域から再生した第3暗号鍵を用いて、上記課金情報を暗号化した第13暗号を第2コンピュータ経由で第3コンピュータへ送る。
873t
n番目の暗号データの第2復号情報を得る
873u
第2復号情報とディスク識別情報と暗号化データnに対して公開鍵系暗号関数を用いた特定の演算を行う
データの平文化
873w
第2コンピュータの処理
873b
第9暗号とディスク識別情報と基本識別情報を受信する
873c
復号鍵データベースからディスク識別情報に対応した通信復号鍵を選択し、第9暗号を復号し、ユーザーデータの平文を得る
873e
ディスク識別情報に対応した第2暗号鍵を暗号鍵データベースから選別し、この第2暗号でサーバーデータを暗号化した第12暗号を第1コンピュータへ送付する
873m
第11暗号を第3コンピュータへ送信
第3コンピュータの処理
873m
新暗号鍵データベースからディスク等の識別情報に対応した第3暗号鍵を探しだし、第13暗号を復号し、課金情報の平文を得る。
873n
課金可能性のチェック
873p
結果を第2コンピュータへ通知
873q
課金可能？
STOP
873r
873s
第n番目の暗号データの第2復号情報鍵を第1コンピュータへ送信
第2コンピュータ

【図24】



フロントページの続き

(72)発明者　田中　伸一
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　小石　健二
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　守屋　充郎
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　竹村　佳也
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Fターム(参考)　5B017 AA03 AA06 BA07 BB09 BB10 CA09 CA16
5D044 AB01 BC03 CC06 DE50 DE52 FG18 GK12 GK17 HH15 HL08
5D090 AA01 BB02 CC04 CC14 DD05 FF09 GG17 GG36
5J104 AA16 NA32 PA14